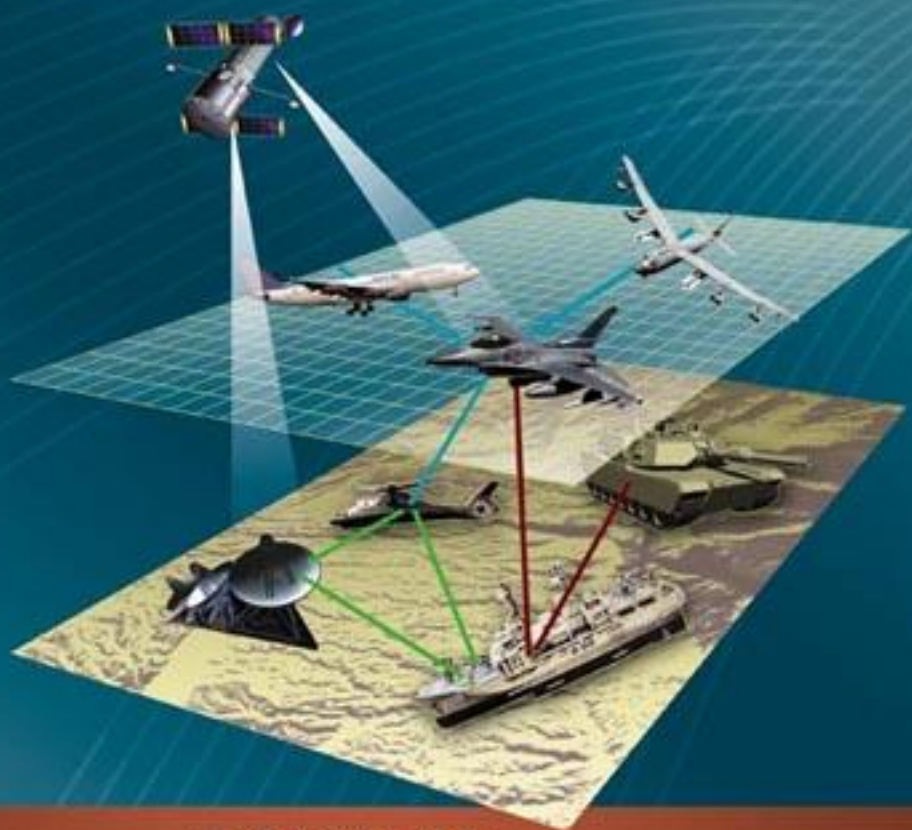


# 军队信息化 理论创新与技术发展

主编 侯喜贵

副主编 董尤心 王积鹏 蓝羽石 刘尔琦



中国电子学会电子系统工程分会第六届学术年会

# 军队信息化理论创新与技术发展

○ 主 编：侯喜贵

○ 副主编：董尤心 王积鹏 蓝羽石 刘尔琦

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

## 内 容 简 介

本书是中国电子学会电子系统工程分会第六届学术年会的论文荟萃,它重点介绍了军队信息化领域的理论创新成果和技术发展趋势,紧密联系我军信息化建设实际,围绕军队信息化建设理论、政策法规、军事信息系统建设以及信息化人才培养等展开学术研讨。全书共分六大部分:军队信息化建设理论研究、军事信息系统综合集成、信息安全保障、信息系统应用开发、信息化人才培养与一体化训练、军队信息化建设关键技术。

本书对国防和军队信息化建设的决策管理、装备科研、人才培养、部队训练等都有很好的参考价值。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

## 图书在版编目(CIP)数据

军队信息化理论创新与技术发展 / 侯喜贵主编. —北京: 电子工业出版社, 2007.11

ISBN 978-7-121-05329-0

I. 军… II. 侯… III. 信息技术—应用—军队建设—研究—中国 IV.E919

中国版本图书馆 CIP 数据核字(2007)第 174620 号

责任编辑: 董亚峰

特约编辑: 时海波

印 刷: 北京季峰印刷有限公司

装 订: 北京季峰印刷有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 880×1 230 1/16 印张: 61 字数: 1 950 千字

印 次: 2007 年 11 月第 1 次印刷

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 [zltts@phei.com.cn](mailto:zltts@phei.com.cn), 盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

服务热线: (010) 88258888。

# 军队信息化理论创新与技术发展

中国电子学会电子系统工程分会

第六届学术年会论文集



# 中国电子学会电子系统工程分会

## 第六届学术年会组织机构

### 领导小组

组 长：侯喜贵

副组长：董尤心    王积鹏    蓝羽石    刘尔琦    符 红

成 员：庄洪林    薛 君    杨建勇    潘学俊    张 宏    管黎峰

曾卫华    潘照年    董晓波    赵冀川    陈克伟    柳晓宏

董满活    王金龙    张维明    刘晓明    曹永林    邵启哲

姚来贵    厉新光    丁晓明    徐 洸    费爱国    宣 民

罗天文    潘旭东    王小非    李恒劭    邓少生    宋跃进

刘克全    张东普

秘书长：戴 浩

副秘书长：陈新中    潘建群

### 学术委员会

主 任：戴 浩

副主任：梁维泰    张毓森    侯卫新    李 辉    张仁茹

委 员：高 岩    罗雪山    曹裕忠    邓建明    李 强    王 强

叶锡庆    胡晓惠    高 扬    梁继民    康炳峰    张 骏

周 武    王小军    缪学宁

### 组织委员会

主 任：王晓明    尹 浩

副主任：张勇丁    陈文生

成 员：孔祥威    汪 林    林 健    刘 进

# 序 言


中国电子学会电子系统工程分会自 1986 年 11 月创建以来，本着共享学术信息、交流研究成果、促进技术合作、普及科学知识、服务军队建设的目的，为推进我军信息化建设发挥了积极作用。

信息化是当今世界发展的大趋势，是世界新军事变革的核心内容。大力推进信息化，是加强国防和军队现代化建设的战略举措，是深入贯彻落实科学发展观，全面履行新世纪新阶段军队历史使命的迫切需要和必然选择。胡锦涛同志在党的十七大报告中深刻指出：要按照建设信息化军队、打赢信息化战争的战略目标，加快机械化和信息化复合发展，积极开展信息化条件下军事训练，加紧培养大批高素质新型军事人才，切实转变战斗力生成模式。近年来，我军信息化建设以科学发展观为重要指导方针，指挥手段建设取得重要突破，武器装备信息化建设步伐明显加快，信息基础设施进一步完善，日常业务信息系统得到普遍应用，呈现出全面发展的良好势头。但我们也要清醒地看到，在我军信息化建设进程中，思想观念创新、理论研究创新、管理体制创新、核心技术自主创新等方面还有很多工作要做。

中国电子学会电子系统工程分会作为推进军队信息化建设的理论研究阵地和技术交流平台，第六届学术年会的主题确定为“军队信息化理论创新与技术发展”，本着理论与实际、当前与长远、继承与创新、需要与可能相结合的原则，紧紧围绕军队信息化建设理论研究、军事信息系统的综合集成、信息安全保障、信息系统应用开发、信息化人才培养与一体化训练、军队信息化建设的关键技术等六个方面开展学术研讨和交流。在分会各团体会员单位和军内外专家学者的大力支持下，本届学术年会共征集论文 581 篇，经学术委员会评审，遴选出 235 篇论文汇编成册。这些论文密切跟踪国内外信息技术的发展趋势，结合本领域学科发展的前沿，着眼前瞻性、突出对策性，研究提出了一些具有创新意义、可操作性强的对策与建议，具有较高的理论研究和实践指导价值，对进一步推进我军信息化建设具有重要参考作用。

本届学术年会由全军信息化工作办公室具体指导，中国电子学会电子系统工程分会主办，总参第六十一研究所和成都军区信息化工作办公室共同承办，各团体会员单位特别是各军区、军兵种、武警司令部通信部，中电科技集团电子科学院、第二十八研究所，中国航天科工集团第二研究院等单位给予了大力支持与协助，在此一并表示衷心感谢！

中国电子学会  
电子系统工程分会主任



二〇〇七年十一月

# 目 录

## 第 1 部分 军队信息化建设理论研究

全面打好基础,推进军队信息化建设 .....	蒋晓原 刘 青 彭慧军 (3)
师旅部队信息化建设研究 .....	黄 艺 (8)
谈军事信息系统装备的特点与发展 .....	徐 洸 周中平 (11)
军队信息化领导管理体制创新初探 .....	符 红 殷 波 (15)
我军信息化规划问题研究 .....	白旭清 马献章 (19)
努力适应应用主导的客观要求积极推进军队信息化建设全面协调发展 .....	张云水 (24)
浅析信息化条件下体系破击作战指挥应具备的几种能力 .....	李广文 李汉琛 (28)
基于电子军务的我军首席信息官制度建设初探 .....	李振富 吴 垚 李旭东 史雅宁 (31)
强化海军指挥信息系统组织运用促进海军战斗力不断提升 .....	魏荣亮 汪海波 李建伟 (35)
对完善我军信息化组织领导体制机制的思考 .....	孙海成 林华生 冯 骞 (39)
军事电子信息系统建设的需求问题浅析 .....	彭慧军 蔡力强 赖 旻 (43)
欧洲军队信息化建设现状与启示 .....	卜格鸿 赵洪利 王英华 (49)
军队信息化发展战略之基本形势和战略方针目标 .....	曹裕忠 林 健 (53)
我军信息化建设的战略思考 .....	鲍国民 聂建平 韩 柯 (57)
信息化条件下维修保障建设构想 .....	陈永龙 徐宗昌 (61)
军用共性软件体系结构研究展望 .....	初 宁 曲向丽 李雪娇 姜 峰 (65)
网络中心环境中 C <sup>4</sup> ISR 作战视图产品描述 .....	邓鹏华 毕义明 刘顺成 (68)
关于加强军事物流系统信息化建设的几点思考 .....	葛 林 傅历光 黄金虎 (72)
美军卫星通信现状、发展趋势及对我军卫星通信发展的启示 .....	郭道省 张邦宁 刘爱军 (75)
对构建海军天基信息应用体制的思考 .....	黄 晖 杨根源 牛利勇 (81)
美俄军队信息化建设基本策略刍议 .....	姜明远 于 滨 (85)
建立军事信息系统灾难备份与恢复体系相关问题思考 .....	李军让 高 岩 宋焱淼 (89)
对比外军发展谈我军信息资源的开发与利用 .....	李 连 李晓奎 邱立军 (93)
军队信息化顶层设计对策分析 .....	李贤玉 王 华 贺 晖 (96)
信息化战争条件下空军作战对后勤保障的要求 .....	高 原 李雪娇 (99)
美国临近空间发展综述 .....	李 铮 程 建 (103)
航天测控技术发展及我们的对策 .....	李志强 张应宪 (106)
军事信息系统装备项目审核管理与评估方法研究 .....	凌孝明 赵纳新 李玉平 (110)
美军运用民用信息技术打造军事信息系统理念对我军影响浅析 .....	王 刚 鲁 岩 程 磊 (114)

用创新机制提升中国软件产业自主创新能力 .....	吕 品	吕家国	(117)
俄军对信息战的研究与准备 .....	庞海东	白永祥	(120)
构建军用软件体系的多视图研究模型 .....	彭治宇	甄 理	(123)
空军信息资源的层次结构与共享分析 .....	邵志平	周中平	(126)
树状信息化建设项目评估体系浅探 .....	隋晓斐	王艳梅	付楚胜 (131)
一种改进的网络节点重要度评估方法 .....	孙 梅	周万宁	詹 武 (134)
军事信息资源目录体系研究 .....	王军玲	荀 静	张红亮 (137)
美军装备保障信息化的现状及发展趋势 .....	徐宗昌	陈永龙	王 军 (142)
军事信息基础设施建设研究 .....		许晓波	(147)
美军联合通信与指挥控制系统建设 .....	杨 茜	李 申	张 灿 (151)
军用计算机网络发展趋势探讨 .....	张 磊	戴 浩	马明凯 刘建军 (155)
信息化条件下我军心理战飞机发展刍议 .....	张 燎	王宣刚	程 建 (159)
信息资源开发利用是军队信息化的核心任务 .....		张新强	任 刚 (162)
一体化联合作战概念牵引美军向信息化军队转型 .....	张永红	陈宇杰	左琳琳 (165)
推动网络中心战, 美国国防信息系统局扮演重要角色 .....	赵 静	孙启辉	(169)
面向服务的军事信息基础网络框架初探 .....	赵为春	徐 卫	马 侃 (174)
信息资源动员建设发展策略探讨 .....	周继文	韩 伟	田 忠 (177)

## 第 2 部分 军事信息系统综合集成

军事电子信息系统综合集成技术 .....		王积鹏	(183)
战区军事信息系统综合集成问题研究 .....		张 宏	(194)
利用建模与模拟支持系统综合的试验评估 .....		施振明	(197)
战术互联网节点编号规则与应用研究 .....	甘志春	李 健	宋贤群 (201)
美军电子信息系统体系结构及其评估方法研究 .....	陈桂生	张新强	彭慧军 李 瑛 (205)
综合集成: 谋求信息时代战斗力的跃升 .....	陈 鹏	孙晋华	曹伟东 张海陆 (210)
军事信息资源共享服务体系建设研究 .....		戴剑伟	吴照林 (213)
分布式网络化作战的复杂网络模型研究 .....	付国宾	谭海涛	沈 宇 (217)
多星遥感任务规划体系框架构想 .....	郭建恩	陈 健	李 湘 王 鹏 (222)
军事信息系统综合集成研究 .....	胡双喜	汤怀松	金家才 (227)
军队指挥信息系统综合集成模式的探讨 .....		李鸿林	杨 涛 (232)
网格环境下分布式异构数据库的数据集成——建立资源描述的本体模型 .....	李君灵	杨晓超	蒋 维 (236)
电子对抗软件工程标准体系的研究与建立 .....		李 强	钟晓峰 (240)
美军 C <sup>4</sup> ISR 体系结构评估方法研究 .....	李 瑛	邹江南	贺 梅 张晓蓓 (246)
分布式网络化作战及其建模 .....	刘宁宁	单维峰	朱 巍 (249)

装备保障信息集成平台框架构建技术研究.....	卢洪义 王文双 史 佩 应新永	(254)
国外防空反导武器系统网络化建设思路与途径分析 .....	施 荣	(258)
信息化条件下装备保障模式初探 .....	时和平 芮科慧 郝 明	(261)
武警信息系统一体化技术体系结构的研究与制订 .....	史国炜 王成海	(264)
野战通信与指控系统装车集成设计技术研究.....	谈学超 张军刚 冯占远	(268)
对临近空间军事开发利用的探讨 .....	王传才 周义建	(273)
浅谈信息作战对炮兵通信的要求 .....	王华命 王 生	(276)
战术数据链的综合集成应用 .....	王启国 曲 悦	(280)
数据资源共享中的交换机制研究.....	胥少卿 罗强一 刘新盛 景柏树	(284)
基于关联矩阵的 C <sup>4</sup> ISR 系统作战体系结构建模研究 .....	徐 佳 顾 健 张祥林	(289)
导弹保障装备测试信息集成系统开发研究.....	于光辉 徐 明 高 山 任海峰 童书辉	(292)
美国防部联合互操作性测试的实施及特点.....	张海翔 邹江南	(295)
数据质量管理的研究与实现 .....	张红亮 罗强一 曹京春	(299)
炮兵指挥信息系统综合集成研究 .....	赵 鑫 闫耀祖 陈 涛	(303)
一种基于智能代理的军事信息系统集成方法.....	周万宁 孙 梅 詹 武	(307)

### 第 3 部分 信息安全保障

军事信息系统安全问题研究.....	厉新光 蒋良艳	(315)
基于 CORBA 的野战指控信息系统安全模型与实现 .....	吕家国 雷武龙	(319)
作战指挥系统信息安全体系结构的思考.....	苗小伟 李殿伟	(323)
军用计算机信息网络系统信息安全对策浅析.....	陈松德	(329)
全面提升新形势下信息网络安全防护能力.....	宁作臣 马建民	(332)
一种军用 RBAC 扩展模型及其实现研究.....	葛方斌 王建新 杨 林	(336)
内网安全不容忽视 .....	石 雄 赵 雯	(341)
建立联合作战可信网络构想 .....	马献章 陈 军 滕明贵	(344)
全面贯彻落实科学发展观努力构建我军信息安全保障体系.....	史正祥 张建辉	(350)
信息化系统抗电磁脉冲方法的研究 .....	常海峰 徐筱麟 王小梅 温怀斌	(354)
军队信息安全保障及技术对策 .....	付仕平 解家宝 徐 飞	(359)
军队信息安全保障体系建设初探 .....	顾正义 孟 娟 胡维益	(362)
移动存储介质安全管理机制的研究与实现.....	郭卫东 谢永强 王朝君 刘 进	(366)
第三代移动通信系统安全体系结构研究.....	郭智恩 谢永强	(370)
可信军用通信网络基础技术 .....	刘建军 顾晓鸣	(374)
电子军务安全与混沌加密 .....	刘 益 郝 明	(378)
两种网管标准的安全性分析 .....	卢 宁 王建新 肖 刚	(381)

军用 Ad Hoc 信息网络的安全威胁及对策 .....	鲁 岩 程 磊 王晨晖 (385)
浅谈我军信息网络安全保障建设 .....	罗 敏 (389)
一种基于代理机制的 RBAC 模型 .....	任 毅 肖治庭 (394)
信息保障需求分析研究 .....	盛丽君 (398)
武警部队信息安全保障系统中的 VPN 技术应用 .....	苏光伟 杨海滨 杨晓元 (403)
战场数据分发系统的授权模型研究 .....	万 鑫 任 毅 (407)
基于异构平台的服务异常检测系统研究 .....	王建伟 谢永强 (411)
美军信息安全防护体系建设情况 .....	王 凯 李 丹 黄海斌 (414)
外军信息保障研究建设现状及启示 .....	王 宁 (419)
对加强我军网络安全应急响应工作的思考 .....	肖治庭 任 毅 岳莹莹 (424)
信息隐藏技术及军事运用浅探 .....	徐新华 黄建冲 (427)
DDOS 攻击技术分析 & 防御策略研究 .....	许 萌 贺 梅 马 烈 (430)
一种提高扩频信号隐蔽性的有效方法 .....	严文超 赵杭生 (434)
基于审计的数据库统计推理攻击发现 .....	袁 震 (438)
指挥信息系统数据中心灾难恢复预案的制定和演练研究 .....	张明安 (442)
一种基于管理员权力限制的数据库安全增强技术 .....	张 锐 刘 军 (448)
基于层次的安全事件关联模型 .....	张潇毅 吴 庆 张 慧 (452)
战场无线传感器网络通信多级安全策略研究 .....	钟俊华 黄曙光 (457)

## 第 4 部分 信息系统应用开发

关注办公文档格式规范 UOF .....	戴 浩 (463)
部队信息资源开发利用情况研究 .....	潘学俊 (466)
地面防空指挥自动化系统研究分析 .....	徐 榕 牟 东 (470)
加强指挥信息系统建设与运用的几点思考 .....	柳晓宏 山 峰 范雄飞 (473)
武警森林部队战术机动综合信息系统构建与应用研究 .....	聂坤华 (476)
强化信息管理能力运作促进军队作战能力提升 .....	梁维泰 (481)
一种基于平流层通信的分层立体化网络组网方式 .....	黄建洋 张洪永 王 靖 (485)
军事通信网络管理系统 .....	莫世禹 李冷冷 (488)
装备维修保障信息的集成化 IETM 系统技术研究 .....	安 钊 徐宗昌 郭红芬 (492)
浅谈信息化联合作战条件下的通信系统组织 .....	毕国平 王作鼎 戴鑫焱 (495)
信息化条件下我军武器装备信息化发展途径探讨 .....	高小玲 卜格鸿 刘力天 (498)
基于复合 Agent 的信息系统模型设计实现 .....	郭天杰 李 瑛 范洪达 (502)
一种通用的基于元数据的异构数据库数据移植技术 .....	蒋国权 严 浩 刁兴春 汪 挺 (505)
野战防空作战中的信息源校准技术 .....	李芳芳 李 新 (510)

舰船装备技术保障信息系统初探 .....	李 峰	曹 原	(517)
基于 HLA 炮兵作战指挥视景仿真系统的设计与实现 .....	李汉琛	李广文	(522)
机载 VLF 中继通信系统探究 .....	李俊清		(527)
基于遗传算法的多 Agent 信息过滤系统研究 .....	李 双	赵怀勋	赵方舟 (532)
军事信息资源开发利用中数据标准化建设问题 .....	李 晓	冯 骞	(536)
基于虚拟现实技术的现代作战模拟系统 .....	梁晓松	许少斌	(539)
指挥信息系统自主管理技术研究 .....	刘必欣	曹 江	张 捷 (543)
图书馆特色数据库建设的理论与实践 .....	刘迎风	曾纲京	(547)
军队信息资源共享的原则与思路 .....	罗永健	杨 鑫	郭 强 郭诗军 (549)
一种全新的国防项目管理信息化服务平台研究 .....	苗 苗	孙 冲	(553)
基于 ANN 的 C <sup>4</sup> ISR 系统数据融合测试评估 .....	那丹彤	赵维康	张子刚 (557)
无线射频技术实现战场维修资源信息一体化 .....	沈云秋	赵韶平	殷维刚 张立新 常 波 (562)
多机空战决策融合实现技术研究 .....	史 进	严丽娜	秦国强 (566)
军校教学保障信息化建设理论与实践研究 .....	孙厚钊	任训平	(570)
基于软构件的军事信息系统的设计与实现 .....	王揽月	平 刚	全洪亮 (574)
军事信息资源目录体系初探 .....	王锐华	张利锋	(577)
做好国防信息化评估, 提升国防信息化建设水平 .....	王顺满	许 楷	(580)
军事装备全寿命信息管理研究 .....	王 增	徐启建	(584)
处置核化事件中指挥信息系统组织运用问题研究 .....	王祖平	高 锋	(587)
区域联合电磁频谱监测管理系统研究 .....	吴 冠	张 超	杨俊明 (591)
基地防御战斗中的电子对抗 .....	巫银花	陆勤夫	陈永芳 (595)
野战通信资源自动配置系统的开发 .....	谢晓霞	史 勇	牛康伟 (599)
信息资源开发利用对策思考 .....	徐 舸		(606)
获取领域知识的本体体系结构的构建 .....	许 勇	王智学	李宗勇 (611)
基于信息融合的装备保障多目标群决策支持系统研究 .....	颜 宁	周 巍	朱晓华 (616)
VS.NET 下信息自动化采集在装备普查中的应用浅析 .....	殷维刚	沈云秋	赵韶平 李 霄 赵曦晶 (621)
OGSA 网格技术在院校信息一体化建设中的应用 .....	由晓民	袁志钢	李艾静 (623)
维修保障交互式电子技术手册 (IETM) 系统建设研究 .....	张瑞丽	李莉华	王向东 (627)
美军新一代战术卫星通信系统—MUOS 系统 .....	张献民	虞明宝	刘爱军 (632)
第三代短波通信网同步管理协议的仿真实现及改进 .....	章锋斌	马大玮	陈正荣 (635)
网络数据存储技术及对大型综合数据库建设的启示 .....	赵 凡	叶锡庆	徐润平 江 帆 (639)
基于探索性分析的军事通信网信息优势 评估指标及框架研究 .....	赵新凯	郭 晶	孔繁东 (643)
无人作战飞机作战应用问题研究 .....	郑晓辉	刘洪坤	(648)
装备保障信息化软件平台建设 .....	朱 敏	高 山	徐 明 于光辉 黄建建 (652)
海战场信息资源组织运用方法研究 .....	朱竹青	黄培荣	(655)

## 第5部分 信息化人才培养与一体化训练

信息化条件下的一体化联合作战训练 .....	符永健 (661)
适应信息化战争需求突出人才队伍建设重点 .....	李治安 (664)
适应新军事变革潮流抓紧工程兵信息化指挥人才培养 .....	徐 波 刘 军 (667)
信息化军事人才的心理素质培养 .....	吴耀光 (670)
关于加强军校研究生信息素质教育的思考 .....	孙继银 何芳芳 王 园 (674)
适应新军事变革努力锻造高素质信息化人才 .....	汤 宁 张波平 (677)
立足推进军事训练转变加强士官教育训练信息化建设 .....	王存才 钱叶平 张文武 (681)
新型军事指挥人才模型建构及培养对策 .....	孙海成 林华生 (684)
以模拟训练为切入点推进一体化训练深入开展 .....	曹光华 洪 宇 (688)
顺应空军战斗力生成模式的转变加快空军信息化人才的培养步伐 .....	程 建 (691)
信息化战场建设与人才问题研究 .....	丁武将 杨雪南 胡思远 (695)
信息化条件下炮兵旅级单位通信建设的几点思考 .....	都迎东 崔 星 (699)
信息化战争条件下军校如何推进现代化教学改革 .....	刘晓宁 宋 绯 邓 莉 (702)
复杂训练仿真系统研究 .....	何 彬 王禹淇 王 琦 (706)
信息化军事人才培养方式探讨 .....	洪 宇 孙 冲 (710)
浅谈一体化训练中的信息化人才培养 .....	华 雪 夏逸平 梁龙喜 (714)
依靠“四个转变”优化院校育才模式 .....	李恩忠 李 彬 张 程 (717)
信息化人才培训应注重强化“五个能力” .....	李科海 韩云山 (720)
加强后勤一体化训练,加快后勤信息化人才培养 .....	李晓燕 孙 云 (722)
联合作战条件下通信兵一体化训练问题的探索 .....	刘齐兵 王新民 (725)
多数据链操作规程研究 .....	罗强一 刘 冰 景柏树 (728)
信息化条件下的一体化训练 .....	彭 超 (732)
积极适应战争形态发展变化努力推进战区一体化训练又好又快发展 .....	戚小光 张继武 王万龙 (735)
信息化条件下装甲兵人才培养浅探 .....	秦 伟 苏 鹏 何 明 (739)
信息化条件下军事人才培养评估 .....	任在安 王 斌 (742)
关于军队信息化人才培养的思考 .....	司维超 李 连 王文才 (746)
浅谈信息化参谋人才的培养 .....	王海源 辛文军 赵东方 (750)
信息化人才信息素质的培养 .....	吴 楠 毕梅冬 (752)
刍议军事院校教学资源优化与共享 .....	杨 莉 刘因海 陈振宇 (756)
以科学发展观为指导,加快信息化条件下军事人才培养 .....	张广忠 全友谊 赵 盼 (759)
中级指挥院校信息化人才培养之浅见 .....	张立新 马远鹏 (763)
浅议侦察情报战线信息化人才培养与一体化训练 .....	赵 磊 (768)
复杂电磁环境下电子对抗部队一体化训练面临的困难与对策 .....	周永生 王峰辉 黄海松 (773)



## 第6部分 军队信息化建设关键技术

军用认知网络技术及其应用研究 .....	王金龙	吴启晖	宋  绯	(779)
矩型码——一种适合地下通信的纠错检错码 .....	司徒梦天	宁志德	方家喜	(783)
谈大型作战方案解算 .....	徐  洸	陈建林		(788)
指挥控制信息系统防御电磁脉冲武器攻击问题研究 .....		李重一		(792)
基于灰色模糊物元的装备保障效能综合评估方法 .....	周  巍	颜  宁	马振江	朱晓华 (796)
数据链与相对时空参照系 .....		徐恩秀		(802)
运用遗传算法实现多星遥感任务规划 .....	陈  健	郭建恩	王  鹏	(805)
基于 WSN 的自动数据采集和处理系统研究 .....	陈贤明	李  俊	蔡跃明	李宗海 曾  文 (809)
战术互联网中基于 MPLS 实现 HMIPv6 的框架模型研究 .....	杜金柱	蒋晓原	杜  磊	(813)
SOA 技术及对军队信息化建设的启示 .....	胡  博	陆余良	徐新华	(816)
移动 GIS 的新应用——位置服务技术 .....		贾  艳		(819)
山区宽带移动战术通信的关键技术 .....	蒋晓红	吕东强	詹  平	(822)
短波 Lorentz 信道确定性仿真模型的设计 .....	李  涛	刘德良	沈  良	谢晓刚 (825)
应用启发式算法解决多星遥感任务规划问题 .....	李  湘	陈  健	靳  峰	朱  博 (831)
数据挖掘技术在军队信息化建设中的应用 .....		李兴生	徐福明	(836)
主动服务和军用分布式数据库应用软件驱动模型研究 .....	李永红	刘东红	罗  睿	姜  峰 (840)
基于 IRP 的军队信息资源开发利用 .....	梁春雨	李振富	李  东	吴  垚 (844)
一种基于小波变换的认知无线电频谱感知方法 .....	林生森	吴启晖	盛雁鸣	(848)
创新的网络体系结构--4D 模型 .....	刘  伟	杨  林	戴  浩	(852)
突发波形在 3G 短波通信中的应用研究 .....	刘振浩	胡中豫	韩  艳	(857)
飞秒脉冲在光子晶体光纤中的传输特性分析 .....	锥开彬	车雅良	何小梅	(862)
基于视觉注意机制的军事遥感图像 ROI 提取 .....	马大玮	李晓飞	陈正荣	凤光华 (866)
协同通信在无线网络融合中的应用方案 .....	潘成康	蔡跃明	徐友云	姜青竹 (870)
基于 BP 神经网络的 C <sup>4</sup> ISR 通信系统效能评估 .....	屈  洋	秦  伟	苏  鹏	(875)
面向高可用网络的 ospf 平稳重启技术研究 .....		商云飞	詹  武	(879)
军事通信网业务流建模及其仿真实现 .....	沈  宇	徐启建	钟  静	陈自卫 (883)
数字化维修技术在陆军航空兵部队应用的初步设想 .....	宋  奕	张  刚	郭  鹏	(888)
一种基于 DDS 的实时信息分发框架 RIDF .....	王  珩	丁  峰		(894)
基于裁剪超宽带 MAC 协议的无线传感器网络 .....	王延峰	李  林		(898)
SAN over SDH 在军事信息网建设中应用研究 .....	王洋洋	廖晓闽		(901)
基于 AHP 和灰色理论的战术通信网系统效能评估方法 .....	韦  涛	田永春		(903)
虚拟化存储技术研究 .....	翁伟兵	吴建国	康东明	(908)
信息化战争条件下的雷达防护 .....	吴爱民	万  福		(913)

基于分数阶傅立叶变换的频谱共享通信方案 .....肖 涵 刘 榕 吴 春 (917)

防空导弹网络化作战关键技术研究 .....熊新平 沈丽艳 宋晋敏 (921)

军事大系统中的监控系统体系结构与关键技术 .....杨雪南 丁武将 (926)

CDMA 军用移动网络安全接入研究 .....叶季青 韩 清 叶酉荪 (931)

基于信号循环平稳特性的智能天线技术.....张洪顺 董明山 陈 磊 (935)

复杂光电环境下激光末制导炮弹作战效能评估方法 .....张 立 周丰平 (940)

体系结构设计方法对军队信息化建设的影响.....张永红 左琳琳 赵利平 席 欢 (944)

基于策略的军事综合网络管理系统研究.....朱 巍 单维峰 易 慧 (949)

基于仿真测试的信息融合能力评估技术研究.....邹 伟 刘 伟 (954)

# 第 1 部分

## 军队信息化建设理论研究

# 全面打好基础，推进军队信息化建设

蒋晓原 刘青 彭慧军

**摘要：**加快推进我军信息化建设，需要在理论和概念、政策、条令、编制、设备、训练、设施、人员等方面全面开展工作，目前急需采用系统工程的形式和方法在上述方面进行基础性的研究和建设。因此，建议由军队信息化工作办公室组织全军有关部门，开展信息化基础工程，打好理论、法规、标准、基础数据、软件应用等方面的基础，有效全面推进全军信息化建设。

**关键词：**军事信息化；基础工程

## 1 以系统工程形式和方法进行信息化基础建设

随着科学技术特别是信息技术的快速发展，人类社会正在快步进入信息社会。在军事领域，信息化的作用也日益凸现，信息化正在世界范围内促进一场新军事变革。纵观世界新军事变革的发展趋势和近期几场局部战争，可以看出，信息化已成为世界主要国家军队建设的方向；信息化改变了战斗力的增长方式，对战争形态演变和军队转型具有决定性作用。各国军队，特别是西方军队，为占领信息化这个制高点，正在积极开展由机械化向信息化的转型，美军的军队转型已有了显著的进展，其在军事领域的优势更加明显、突出。军事信息化的实质就是将信息技术渗入各种军事系统，并将信息采集和处理全面融入各种军事应用，使军队作战能力和管理水平提高到一个全新的高度。

经过二十多年指挥自动化建设，为我军信息化建设打下了基本的技术和物资基础，全军信息化领导小组的成立，标志着我军信息化建设已进入全面发展的阶段。总结我军信息化建设的经验和借鉴美军信息化的历程，可以看出，信息技术、装备（设备）和系统建设是信息化建设的主要组成部分，在理论和概念、政策法规、编制、设备、训练培训、设施、人员等方面的建设也是必不可少的重要部分。目前全军各级对信息系统的建设不能说不重视，经费和装备投入不能说不高，但是在整体效果上仍令人普遍感到不满意，其原因在于与信息系统建设和使用配套的理论概念、政策法规、编制、设备、训练培训、设施、人员等方面的工作基础薄弱，严重滞后于信息装备和系统的建设。

为了适应信息化作战和管理的需要，在更高的层次上加快推进我军信息化建设全面发展，目前急需解决制约我军信息化发展的重点、难点问题，这就是：必须从理论和概念、政策法规、编制、设备、训练、设施、人员等方面全面打牢发展基础，才可能提高我军信息资源开发水平和使用效率，加快我军信息化全面建设进程。

因此，需要以江泽民国防和军队建设思想、胡主席一系列重要指示为指导，全面贯彻落实科学发展观，以新时期军事战略方针为统揽，以《军队信息化规划纲要》为依据，以信息资源开发利用为主线，以跨领域、跨部门的信息化基础性工作为重点，以既设信息基础设施和国家信息化建设成果为依托，立足现有体制，切实发挥全军信息化工作体系的职能作用，依靠全军力量，采用系统工程的形式和方法，整合现有资源，填补基础方面的空白，大力推广信息化成果，提高应用水平，促进体制机制完善和战斗力生成模式转变，为我军信息化全面、协调、可持续发展打牢基础、创造条件。

## 2 对开展信息化基础工程的建议

信息化基础工程应着眼我军信息化建设全面协调可持续发展实际需要，对影响军队信息化进程的各项基础性工作进行统筹规划，合理安排，深入推动理论研究、需求论证、标准体系、政策法规、数据建设、信息安全和应用软件开发等跨领域、跨部门的信息化基础性研究和建设工作，并为指导和规范我军信息化建设提供公用支持手段和示范系统。我军在这几个跨领域、跨部门的基础领域已有一定积累，形成了一些成果，但仍然还有许多重难点问

题，需要汇集全军智慧、整合各方面力量才能加以解决。

2.1 建设目标

紧紧围绕我军信息化工作的重难点问题和薄弱环节，通过开展信息化基础工程建设，在“十一五”期间，形成信息化理论体系，明确信息化顶层需求，建立信息化标准体系，填补信息安全基础设施中的空白、完善安全保障体系，整合全军基础数据标准和资源，建成总部到各大单位的通用日常业务信息系统，为全军信息化建设打下坚实的基础。在“十一五”期间，基本完成如下基础工程建设。

- 建立四个体系：信息化理论、信息化法规、信息化标准和信息安全保障体系；
- 提供方法与工具：需求论证、标准化产品

验证、安全风险评估与检测、数据集成与共享、应用软件构件重用和网络化办公等方法与工具（软件）；

- 统一基础数据资源：全军人员基础数据、全军组织机构基础数据、全军通用物资基础数据、全军装备基础数据、国防设施基础数据；
- 建成两个示范系统：全军人员基础信息管理系统和通用日常业务信息系统。

2.2 信息化基础工程的体系结构

信息化基础工程的体系结构如图 1 所示，由总体进行系统结构的顶层设计，使信息化基础工程的各项项目相互支持、配合，形成有机的整体。

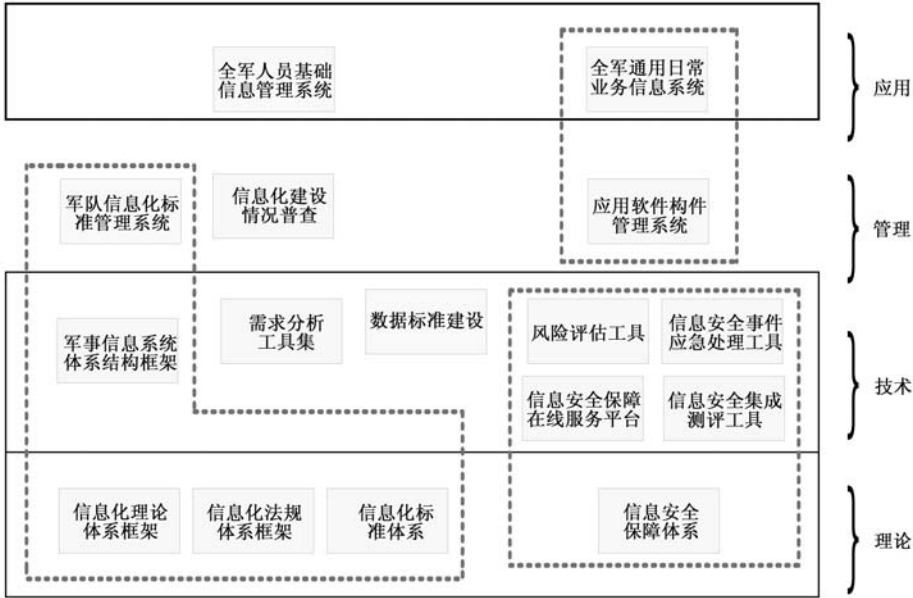


图 1 信息化基础工程系统结构图

如图 1 所示，信息化基础工程体系结构可分为理论基础、技术基础、管理基础和应用示范四个层次。

1) 在理论基础层，要建立信息化理论、法规、标准和安全保障体系框架，并逐步形成一系列的理论、法规和标准成果，从观念、条令、编制、训练、装备、设施等方面全面指导和规范全军的信息化工作。

2) 在技术基础层，一方面要建立军事信息系统体系结构框架，统一全军各类信息系统的分析、设计、研究方法和信息化公共参考资源，确保全军

信息化建设按一体化的方向发展；另一方面主要是填补信息化技术支持环境中的空白和薄弱环节，提供需求论证分析工具、基础数据标准，以及有关信息安全的风险评估、应急处理、在线服务和集成评测等工具，统一需求分析、数据共享和信息安全方面的技术体制，为管理和应用层提供支撑和服务，提高全军信息化建设的基础技术水平。

3) 在管理基础层，要建立军队信息化标准管理系统、国防数据词典系统和应用软件构件管理系统，实现对信息化标准、国防数据词典、应用软件构件等进行科学、规范化的管理，为全军信息化建

设提供有效的服务。

4) 在应用层,充分利用理论、技术、管理基础层的支持,以全军人员基础信息管理系统和全军通用日常业务信息系统作为信息化建设推进的试点,完成二个应用系统的开发和建设,并全面检验信息化基础工程的成果。

## 2.3 内部关系

信息化理论建设要及时提供,直接指导总体和各项项目的科研和建设,为信息化基础工程成果的推广应用提供理论依据。

需求工具建设要为总体和各项项目的需求研究的全过程提供方法、工具和基础资源的支持,使提交的所有需求论证报告都符合相关的标准,对这些需求论证报告的一致性、正确性、完整性进行验证。

信息化标准建设要建立信息化标准体系,用军事信息系统一体化技术体系结构(ITA)指导各项项目的标准制定、管理和宣贯,对各项项目提交的标准进行验证。

信息安全保障体系建设要确定基础工程的信息安全要求和实施方案,提出可信安全环境的要求,确定人员基础信息管理系统和通用日常业务信息系统的信息安全等级,进行信息安全风险评估,提供网络信任支撑技术和工具,构建安全事件应急响应体系。

数据标准建设要建立数据标准体系,为通用日常业务信息系统提供数据标准、数据支撑环境和数据集成与共享工具,统一全军人员基础数据、全军组织机构基础数据、全军通用物资基础数据、全军装备基础数据、国防设施基础数据,通过人员基础信息管理系统和通用日常业务信息系统建设进行示范,验证基础数据标准体制。

通用日常业务信息系统要建立网络化日常业务信息系统架构,提供共用办公业务软件,充分利用其他项目的成果,建成试点应用系统,综合体现基础工程的科研和建设效果。

基础工程的各项项目制定的理论、法规、标准、方法、工具、应用系统等成果,要直接在基础工程的其他项目中提供应用,并在使用中不断完善,同时还要在全军推广应用,为我军信息化建设提供基础性的支持。

## 2.4 与外部系统的关系

信息化基础工程的理论基础、技术基础、管理基础层也应成为整个军事信息系统的基础,除了能够支持上图应用层的两个典型应用外,今后还要支持包括指挥控制系统、武器信息化系统、支援保障系统等在内的各种军事应用系统。但是,信息化基础工程前期确定的建设内容,还不能构成完整的信息化基础体系,因此,信息化基础工程也需要充分吸纳和采用全军已有的信息化建设成果和现有的信息基础设施,相互补充,相辅相成,以形成比较完整的信息化基础体系。

# 3 信息化基础工程的主要建设内容

## 3.1 工程总体工作

工程总体工作除了总体方案论证、计划管理与协调工作以外,重点进行信息化建设总体研究和普查分析工作。

### 3.1.1 信息化建设总体研究

主要开展军事信息系统体系结构、信息化理论、信息化法规、信息化评价方法与指标,以及信息化标准体系的研究工作。通过信息化建设总体研究工作,建立我军信息化体系结构框架、信息化理论体系框架、信息化法规体系框架和信息化评价体系;更新升级军事信息系统一体化技术体系结构(ITA),利用网络技术提高信息化标准管理与服务水平,推动相关标准产品化。

### 3.1.2 普查分析

开展军事信息系统应用情况和信息资源情况的普查,制定普查方案,开发普查软件,组织普查结果分析,形成能准确反映当前我军信息化建设实际需求和存在问题的普查报告。在获得的普查数据的基础上,建立全军信息化基础数据库,为信息化决策提供科学的数据依据。

## 3.2 需求论证工具和参考资源建设

需求论证工具和参考资源建设主要是研究军事需求分析论证基础理论,制定需求论证有关法规标准,开发研制需求分析论证工具和需求论证基础资

源, 规范和支持军事信息系统和信息化武器装备建设的需求论证分析工作。

### 3.2.1 需求论证工具

分析研究国内外需求论证理论方法和技术手段, 针对不同层次、不同类型的需求论证工作, 采用优选成熟商业产品、改造升级现有预研成果和新研空缺工具相结合的方式, 集成一套完整、规范的需求获取、描述、验证和管理等需求分析论证工具; 开发需求论证基础资源、需求分析论证工具集成软件, 在统一的平台上为需求开发和管理人员提供辅助支持和需求验证功能; 在平台建设、全军人员基础信息管理系统建设和全军通用日常业务信息系统建设中, 试点应用需求分析论证工具; 组织推广需求分析论证工具, 制作需求工具软件包, 配发全军各大单位。

### 3.2.2 参考资料

以联合作战需求为牵引, 全面论证联合作战任务清单的概念、内涵、组成和作用, 研究联合作战任务清单编制规则, 编制我军信息化条件下联合作战任务清单; 开发需求分析论证模板库, 为需求获取、描述、验证和管理各阶段提供常用的需求开发数据与模型、需求开发规则与模板、需求验证指标与评估模型等。

## 3.3 军队基础数据标准建设

军队基础数据建设主要工作是制定数据管理规定, 统一基础数据标准, 促进全军数据资源整合, 实现数据统一管理、按需共享。

### 3.3.1 基础数据标准和法规

制定军队数据管理规定, 论证拟制《全军数据资源建设总体规划》, 全面统筹、规范我军基础数据资源建设; 编制数据标准体系表和全军数据标准编制规则, 制定数据质量控制标准, 明确我军数据标准化建设总体框架、发展目标和质量要求; 论证提出我军数据共享交换的技术体制, 为信息化基础工程有关项目建设提供理论依据。

### 3.3.2 国防数据词典系统

以现有作战数据标准建设成果为基础, 统一全军人员、组织机构、物资和装备的数据元素标准、

分类编码标准、数据结构标准和元数据标准, 吸收侦察情报、地理空间、气象水文等基础数据标准, 建立国防数据词典; 依托军事综合信息网建立国防数据词典系统, 用于维护、管理国防数据词典, 并支持各级数据管理部门利用国防数据词典系统开展数据管理和应用工作, 支持授权用户查询和下载标准数据和数据结构。

### 3.3.3 基础数据资源

在统一全军人员、组织机构数据标准的基础上, 统一组织、分工采集(抽取)全军人员、组织机构基础数据, 改造相关业务数据库, 建立并充实全军人员、组织机构基础数据库, 为全军有关业务部门使用人员、组织机构提供基础数据服务。

## 3.4 信息安全保障体系建设

以构建我军完整的信息安全保障体系为目标, 开展信息安全战略研究, 组织信息安全风险评估、等级防护、应急处理、可信计算的法规标准制定和工具手段建设, 填补信息安全保障体系建设空白, 开发信息安全在线服务平台, 逐步建立全军信息安全网络服务体系。

### 3.4.1 信息安全总体研究

开展我军信息安全战略研究, 拟制《信息安全保障体系总体设计报告》, 明确我军信息安全保障的概念、内涵、组成和相互关系, 为开展军队信息安全保障建设奠定理论基础; 以在役保密设备和系统安全设备为重点, 借鉴各类信息系统安全防护配套建设经验, 制定信息系统安全系统配置指南, 为各类新研信息系统的安全系统配套建设提供指导; 开展等级保护总体研究, 探索军队信息系统等级保护工作分工与组织实施办法, 制定相关法规标准; 研究提出符合我军军事需求的可信计算体系结构, 指导可信硬件设备和软件产品的研制开发工作。

### 3.4.2 信息安全工具手段

制定军队信息安全风险评估相关法规标准, 规范信息安全风险评估的工作流程、评估内容、评估方法和风险判断准则, 研制信息系统安全性分析、密码安全风险分析、软件逆向分析、信息系统渗透性监测工具, 建立风险评估管理系统和风险评估支撑数据库, 为开展我军信息安全风险评估工作提供

依据和工具手段；建立健全军队信息安全应急处理法规标准和有关制度，规范信息安全事件应急处理方法、流程，开发信息安全事件取证、预警、定位、备份恢复等应急处理工具和协作响应平台，为信息安全事件处置提供必要的手段，为构建我军信息安全应急处理体系奠定基础；开发或改造安全产品入网监测和系统集成测评工具，支持安全产品和信息系统测评与管理工作。

### 3.4.3 信息安全保障示范系统

依托全军人员基础信息管理系统和全军通用日常业务信息系统开展信息安全保障示范系统建设，利用等级防护建设成果，对应用系统进行等级确认；利用风险评估工具和管理平台，对系统进行风险评估，形成评估意见；由第三方组织网络攻击等入侵试验，利用应急处理工具和响应平台，进行信息安全事件应急处置。通过典型示范系统建设，全面检验工程建设成果，形成军队信息系统安全防护、身份认证、授权管理等方面的典型配置、工作机制和应用方案。

### 3.4.4 信息安全保障服务

开发军队信息安全保障在线服务平台，依托军事综合信息网，建立信息安全网络服务体系，为全军各级、各部门提供病毒通报、漏洞补丁、安全系统更新、升级等信息安全服务。

## 3.5 全军人员基础信息管理系统

制定人员基础信息建设、管理和使用法规，统一全军人员和组织结构基础数据标准，整合改造与人员基础信息有关的信息系统，实现全军人员基础

数据“一数一源”、集中管理和信息按需授权共享，解决我军军事、政治、后勤三大实力统计系统中人员数据统一的问题，完成全军士兵和干部基础数据建设，组织实施数字化军人证件试点建设。

## 3.6 全军通用日常业务信息系统

调研全军业务处理软件建设和应用现状，总结建设经验，组织软件优选，研究确定系统功能和技术体制，建立全军应用软件体系结构框架，统一通用信息处理平台和共用支撑软件。制定全军应用软件构件资源建设总体规划，制定应用软件构件标准和有关管理规程，开发构件资源管理系统，依托未来的平台和通用日常业务信息系统建设成果，试点建设指挥控制类和通用日常业务类构件资源库，开发构件库在线服务系统，为用户提供构件信息的发布、浏览、检索，以及构件上传与下载等网络化服务和技术支持。在此基础上，集成优秀软件模块，开发全军通用日常办公软件，提供公文处理、信息服务、事务管理和文档管理等工具手段，组织在全军各大单位推广通用日常办公信息系统，“十一五”期间，基本实现总部各业务部门之间、总部与各大单位之间信息交互、业务协同。

遴选符合软件企业资质认定的优秀软件企业，定制适合军队需求、具有自主知识产权的字处理、电子表格、演示文稿等国产软件。在此基础上，定制具有协同办公、电子邮件和即时消息等功能，拥有自主知识产权的办公软件协作平台；选择军内信息化基础较好、应用水平较高的试点单位进行试用，检验定制产品的实用性和可靠性，为在总部、全军各大单位推广应用奠定基础。

参考文献（略）

### 作者联系方式

通信地址：北京丰台大成路13号

邮政编码：100039

联系电话：010-66820013



# 师旅部队信息化建设研究

黄艺

**摘 要：**师旅部队作为我军的基本战术兵团，其信息化建设水平在军队信息化建设中具有举足轻重的作用。如何正确指导师旅部队信息化建设，努力实现师旅部队信息化建设的突破性进展，为军队信息化做出应有的贡献，是必须回答和解决的重大问题。

**关键词：**信息化；部队建设；师旅部队

## 1 科学规划师旅部队信息化建设的目标和任务

推进师旅部队信息化建设，实现师旅部队信息化，是一项科技含量大、涉及范围广、一体化程度高、时间跨度长的系统工程，决不是“一哄而起”的盲目建设所能实现的。必须在部队党委、首长的统一领导下，从战略高度进行科学的顶层设计，合理地规划建设目标和任务，分阶段有步骤地实施。

### 1.1 规划师旅部队信息化建设目标的主要依据

规划师旅部队信息化建设的目标和任务，必须依据未来信息化战争的发展趋势、军事斗争的客观需求、军队现代化特别是信息化建设发展战略、部队建设的现状和信息化建设的客观规律等进行科学运筹。特别应把握好以下几点：一是部队担负的军事斗争任务。加强部队信息化建设的根本目的，是提高军队的履职能力，打赢可能发生的高技术局部战争。因此，师旅部队信息化建设一定要以作战需求为依据，充分考虑部队所担负的作战任务的需要，以及未来信息战特点对部队信息作战能力的要求。二是军队信息化建设发展战略。师旅部队信息化建设必须坚持局部服从全局的原则，符合我军信息化建设“三步走”的发展战略，按照军委的统一部署从长计议，当前主要应在打牢信息化建设的基础上下功夫。三是部队建设的客观实际。目前，我军师旅部队的信息化水平很低，武器装备处在机械化、半机械化阶段，信息网络不够完善且性能较差，信息资源的开发利用尚处在启动阶段，人才的信息化素质相差甚远。师旅部队在计划信息化建设

时，应该考虑到这些客观实际。四是军队信息化建设的基本规律。军队信息化建设有其自身的特点和规律，如从建设要素的内在关系上讲，军用信息网络的建设是基础，指挥自动化系统建设是核心，军用资源的开发利用是重点，武器装备建设是标志，各类军事人才的培养是关键。在谋划师旅部队信息化建设时，这些都是必须认真把握的。

### 1.2 对师旅部队信息化建设近期目标的设想

师旅部队信息化建设尚处在起步阶段，因此首先应科学确定其近期目标和任务，重点解决“有与无”、“多与少”和“高与低”的问题。初步设想，师旅部队近期（主要是近五年）信息化建设的目标应是：全面启动师旅部队信息化建设工程，狠抓信息基础设施建设和人才培养，有计划地提高机械化水平，并推进武器装备信息化改造，有效地开发利用信息资源，促进部队信息作战能力的明显提高。

#### 1.2.1 建成初具规模的军事信息网络

实现营区网上信息的实时传递与共享，为办公自动化和网络化训练提供较先进的信息化平台；力争使野战信息网络覆盖作战地区，实现作战信息的实时传递与共享，为提高部队信息作战能力提供较先进的信息化平台。

#### 1.2.2 建成具有相当规模的信息资源库

主要是建成部队作战编成信息数据子库、武器装备信息数据子库、作战环境信息数据子库、战场态势信息数据子库、作战情报信息数据子库、部队教育训练数据子库等，实现师旅部队各类作战与工作数据信息共享。

### 1.2.3 武器装备信息控制能力明显提高

主要是在发展机械化武器装备的基础上,积极运用信息技术和信息网络,对现有武器装备进行力所能及的信息化改造,提高对武器装备的信息控制能力。

### 1.2.4 “电子军务”得到较普遍的应用

主要是使计算机“无纸化”办公普及化,逐步实现师旅部队军事、政治、后勤、装备等部门的办公业务和其他信息服务网络化。

### 1.2.5 信息化人才队伍基本形成

主要是部队官兵的信息化意识普遍增强,信息科技知识水平普遍提高,特别是指挥员的信息作战指挥水平及信息系统官兵对信息系统的使用管理能力明显提高,适应部队信息化建设需要的信息工程技术队伍基本形成。

### 1.2.6 信息化活动完全纳入法制化轨道

主要是在各类信息化活动中,严格遵守和执行总部颁发的各项信息化政策法规和标准规范,特别是有关信息安全保密的各项法规;根据部队信息化建设需要,制定一些具体的规章制度和操作规程,确保部队信息化建设健康、有序地发展。

## 2 突出师旅级信息化建设的重点

### 2.1 加强指挥信息系统建设

当前,世界各国军队在信息化建设上都十分重视以指挥控制为中心的  $C^4ISR$  的建设,将各种信息化武器系统、作战平台,电子装备和信息化人员综合集成为一体化的信息化作战系统,使战斗力得到倍增。建立常驻地及预定作战地域指挥控制系统,为构建信息化战场奠定基础,为信息化指挥控制提供支撑平台。为此,要在预定作战地域侦察监视系统、情况报知系统和信息传输系统拓展的基础上,以数字化设备为接口,通过通信传输系统将指挥控制与侦察监视系统、情况报知系统联为一体,以支持指挥控制人员、作战执勤人员和保障人员的信息活动,有效地缩短获取信息、处理信息和采取行动的时间;对所获得的战场信息进行统一协调、综合处理,筛选识别、分析利用和实时控制;连通部队

各级、覆盖各层、传输综合信息,形成战场信息资源的共享和信息的交换;有效地加强各级部队之间、一线部队之间的协同,简化指挥程序,提高边防部队的快速反应能力,进而实现指挥实时化,侦察、打击(处置)一体化的目标。

### 2.2 加强综合保障系统建设

目前,许多国家在整体军事力量建设的提升时,都注重考虑到了综合保障的配套与协调发展问题,并将其保障列入军队发展的总体规划。首先,要注重保障的系列化、通用化、整体化发展。如美国陆军的信息化指挥控制、后勤、装备保障中,都十分注重“三化”建设,通过海湾战争等局部战争的检验,均发挥了很好的作用。其次,要对现有有保障模式和手段进行技术化、信息化、更新化改造。如美军将先进的微电子技术和数字通信技术用于陈旧装备改造,以弥补新装备不足的问题,这样既可节省经费,又能迅速提高技术保障装备的层次和保障效率。实际上,进行信息化作战的数字化部队,不仅需要大量的技术力量来进行技术保障,同时还要及时提供各种后勤、装备保障服务,以此确保部队的训练、演习、作战以及生活的有序进行。

### 2.3 加强武器装备信息化建设

武器装备的现代化是信息化建设的物质基础。目前,我军武器装备离信息化要求还有很大的距离。部队指战员应立足现有武器装备水平和条件,结合实际,虽然对配发的信息化武器装备和现有武器装备进行信息化改造,主要靠上级装备部门实现,但师旅部队也是可以有所作为的。当前应突出抓好“三个强化”,即强化对现装机械化装备的综合运用,强化信息对火力的控制能力,强化武器系统的“横向一体”,以此来提高武器装备的整体作战能力。

## 3 努力实现师旅部队信息化建设的若干建议

师旅部队为实现信息化建设的目标和任务,尽快实现信息化建设的突破,必须在狠抓思想观念更新、增强信息化意识的基础上,采取有效的对策措施。

### 3.1 狠抓信息基础设施的建设，打牢信息化建设基础

信息设施是信息化建设的基础工程，必须放在优先发展的地位。考虑到师旅部队的客观实际和作战需求，当前应重点抓好“三大工程”建设：一是信息网络工程建设。主要是通过加大投入加快建设，力争使通信网络连到班以上作战单位，部队局域网连接到连以上单位，可视电话会议系统进入连队。二是指挥自动化工程建设。主要是在上级配发的相应装备的基础上，通过积极努力，不断提高部队作战指挥的自动化水平。三是信息资源开发工程建设。主要是组织力量进行信息资源开发，力争早日建成部队信息资源库，实现各类信息资源的数字化。

### 3.2 狠抓信息化人才培养，建设信息化人才队伍

加快部队信息化建设，不断促进我军现代化建设向信息化跨越，人才是关键。信息化人才是部队信息化建设的决定性因素，也是师旅部队大有作为的建设工程。着眼当前的迫切需求，应重点培养好“三支队伍”：一是指挥员队伍。现代高技术战争的复杂性，以及武器装备科技含量的不断提高，要求师旅级干部不仅能指挥、善管理，而且要懂技

术。因此，应通过交叉培训、换岗锻炼等形式，尽快使他们具备以现代信息技术为主体的多维知识结构，以信息作战理论为基础的较高军事素养，以信息作战能力为核心的联合作战组织指挥能力。二是信息工程技术人员队伍。下大力培养和引进人材，努力打造高水平工程技术队伍，以便更好地规划、建设、开发和管理信息化系统。三是信息系统队伍。全面提高包括通信兵、电子对抗兵、侦察兵、机要兵在内的信息系统队伍的信息化素质，充分发挥其在信息化建设中的主力军作用。

### 3.3 狠抓信息化实践活动的开展，强化官兵的信息素质

师旅部队信息化水平的提高，不仅要有信息化的物质基础，而且要靠信息化实践活动的锤炼。可通过开展“三上活动”，强化部队官兵的信息素质。一是“上机”活动，即通过普遍的计算机操作使用、运用计算机办公等实践活动，提高广大官兵使用计算机的水平和能力。二是“上网”活动，即通过普遍上“军队教育训练网”的实践活动，提高广大官兵网上浏览信息、查询信息、传递信息的能力。三是“上场”活动，即通过组织广大官兵在信息化模拟化训练场进行信息装备武器系统的操作使用训练、信息对抗训练和其他联合作战训练，提高他们的信息作战能力。

参考文献（略）

作者联系方式

通信地址：云南昆明 77200 部队

邮政编码：650032

联系电话：0871—47770303

# 谈军事信息系统装备的特点与发展

徐洸 周中平

**摘 要：**军事信息系统装备作为实施联合作战组织指挥的重要手段，已成为各国军队装备体系中的重要组成部分，本文从包含军事信息系统在内的大装备观和软装备观出发，对比分析了军事信息系统与常规武器系统装备的不同之处，在归纳军事信息系统装备本质特征的基础上，提出了具有军事信息系统装备特色的发展要求。

**关键词：**军事信息系统；信息化装备；发展策略

随着军队信息化建设的深入发展，军事信息系统装备已成为我军装备体系中的重要组成部分，而且作为实施联合作战和信息作战指挥控制的物质基础和重要手段，其作用和地位日益突出。树立起包括军事信息系统在内的大装备观，认真研究其本质特征和特殊的建设发展要求，对信息化条件下军队装备体系的完善是有着重要意义。

## 1 军事信息系统是信息化装备的重要组成部分

### 1.1 军事装备信息化发展的三个层面

在军事装备领域其信息化的发展过程基本上可以反映在三个层面。

第一个层面：武器平台的信息化改造。这是指在原机械化武器装备、电子武器装备的基础上进行信息化功能扩展而成为信息化作战平台，各种传统的常规武器平台（飞机、舰艇、坦克等）在经过数字化、智能化改造后，使之成为具有较高信息化程度的武器平台。

第二个层面：信息化装备的快速发展。这里信息化装备是指具有收集或获取、传输、处理信息单项或几项功能的具体装备，以及对敌方信息系统与设施起到有效干扰、压制、破坏和摧毁作用的武器系统，包括各种信息探测装备、信息传输和处理设备、信息制导和遥感武器等，如雷达、地面传感器、夜视器材、声纳、通信装备、精确制导武器、遥感炮弹、高功率微波武器、激光武器、电磁脉冲武器、计算机病毒武器等。

第三个层面：是指挥控制领域的信息化。即在军队指挥体系中发展智能化、自动化、一体化的军

事信息系统，提高指挥效能，使兵力兵器得到合理的配置和有效的使用，释放出最大的作战效能，充分发挥各种武器平台的整体作战能力，起“兵力倍增器”的作用。

从以上三个层面的内容看，前两个层面指本身具有信息获取、传输、处理等一项或多项功能的武器装备，是传统的武器装备范畴，而第三个层面的功能则主要涉及作战指挥领域的信息，是正在逐步扩展的装备范畴。时代发展到今天，应该形成一个基本共识：即装备信息化既包括作战武器装备的信息化，也包括指挥控制装备的信息化；而且对于对作战效能产生重大影响的作战军事信息系统，应该列入装备信息化建设体系的重点发展领域。

### 1.2 军事信息系统属于军事装备的范畴体系

根据军事装备学的概念界定，“装备”是用以实施和保障军事行动的武器、武器系统和其他军事技术器材的统称。对于军事信息系统，它可以归属于广义的武器系统的范畴。一是随着各种武器平台信息化程度的提高，指挥控制与各种兵器的交链越来越紧密，战术级的军事信息系统既是保障各类信息化武器军事行动的“中枢神经”，也逐步成为武器实体的一部分；二是军事信息系统是取得信息优势的必备条件，未来战争中“制信息权”将是作战争夺的“焦点”，信息战的攻击力量和攻击目标主要在网络化的军事信息系统上展开，所以它已经不仅仅是指挥工具，而且还是实施信息战的主要平台、指挥控制战的主体，即信息系统武器化的趋势十分明显；三是军事信息系统的“粘合”作用，现代飞机、舰艇、导弹、雷达等信息化武器平台，它们还只是“个体化”的信息探测、传输、处理和使用单位，要实现以上各个体之间的信息资源共享，

必须把它们与指挥机构及作战部队置于一一体化的军事信息系统的统一指挥控制之下，这样才能使信息、信息武器装备和作战部队、支援保障部门的效能得以充分发挥，在作战运用中完成“个体化”信息武器装备所无法完成的任务，使整体使用效能远远大于各个“个体化”信息武器装备使用效能的简单叠加。

军事信息系统是一种智能化的信息处理系统，能够快速将搜集到的各类情报比较、判定、融合，并制定出作战方案，为指挥机构和指挥员提供高效率的辅助决策服务，能在极短的时间内将作战指令分发到所属的兵力兵器，使有关的力量快速进入战备状态，使决策指挥与控制兵力兵器实施作战行动几乎同步。由于军事装备是生产工具在军事领域的对应物，它随着科学技术的进步、社会生产力的提高和战争的需要而不断发展。在信息化条件下，我们认为军事装备的特色既应该体现在武器装备的信

息化程度方面，也应该反映在典型的信息化武器装备方面。近几场局部战争已极大地呈现出了武器系统信息化、信息系统武器化的特征。因此对于装备范畴的认识必须随着时代的变革而发展，军事信息系统作为特殊的武器系统，正在发展成为军事装备体系的重要成分。

2 军事信息系统具有与常规武器系统不尽相同的装备特性

信息化程度逐步提高的战斗机、舰艇、导弹等武器系统平台，与军事信息系统有某些相同特点，如都引入了以计算机为代表的信息处理和自动控制装置。但通过分析比较就会发现，两种装备的客观环境和用户的主观要求都有非常大的不同之处（见表1）。

表 1 军事信息系统与常规武器系统的区别

	军事信息系统	武器系统
同时生产数量	单个或少量	批量或大量
使用需求	不确定因素多，变化很大	较明确、具体，变化较小
使用人员的种类	指挥员、参谋为主，战勤操作人员为辅	主要是战勤人员
硬件研制	可较多地利用现有实用的高技术产品	有特定的需求，专门研制
计算机	通用机及少量专用机	专用机
接口关系	复杂	相对简单
软件工作量及所占费用比重	很大	较小
对软件人员的需求	需要专职的软件人员保障	对软件人员的依赖性较小
同时使用人员的数量	较多	较少
交付使用后改进的可能性	很大	很小
使用期间的变化	不断有部分软硬设备改进、更新	有明显的换代标志，新旧更替

分析军事信息系统的本质特性，可以看出其特殊性在于与作战指挥的密切相关性和软件系统集成

的关键性。

2.1 军事信息系统是一种典型的人-机系统

它是高技术与军事指挥要求紧密结合的产物，指挥参谋人员在系统中处于特殊的地位，是系统在发挥功能的过程中非常关键的一环。由于军事信息系统的主要用户是指挥员和参谋人员，因此指挥参谋人员对系统的需求、理解以及在指挥决策过程中的运用水平，对系统效能的发挥至关重要。作为指

挥员对部队及武器装备实施指挥控制的手段，它具有高度智能化的辅助决策功能。常规的武器系统以硬设备为主，辅以少量的结构化或半结构化的信息处理和

控制软件；而在军事信息系统中，重头戏恰恰在面向指挥决策的应用层面，作战应用软件尤其是辅助决策软件占有相当大的比重（美军已占系统总研制费用的 50% 以上）和极其重要的位置。

2.2 军事信息系统的需求和功能都有一个渐进获取的过程

常规武器系统的功能在一个时期内可以比较稳

定,有明显的更新换代标志,通常是批量生产;每一个具体的军事信息系统都是特定的军事需求和特定的技术相结合的产物,而且军事信息系统在运用中功能的扩展和改进是不可避免且频繁的。一方面,军事需求随着技术的更新和指挥参谋人员对系统认识的不断深入而迅速变化;另一方面,军事信息系统的建立目标(功能和性能)及使用效益也是逐渐获得的。因此强调在系统的组织实施和使用中不断改进、不断完善、不断提高效益。

### 2.3 军事信息系统的研制与作战指挥理论、作战样式密切相关

系统研究的对象主要是指指挥所需的信息及其在指挥体系中的活动规律,因此系统功能以及作战应用软件都紧随作战思想和指挥理论的变革,同步发展富有活力。军事信息系统的组织运用过程,是紧紧围绕对指挥所需信息的收集、传递和处理,以及如何利用这些信息进行指挥决策和控制而展开的,这与常规武器系统的运用和维护有明显的区别。

综上所述,军事信息系统是一种十分特殊的武器装备,它是一种支撑指挥决策和控制的信息系统,是多种设备和作战应用软件的综合集成,并且这种综合集成远不是单纯的技术问题,而是要体现出一种全新的为作战意图服务的系统观念。

## 3 根据军事信息系统装备特点把握建设要求

从军事信息系统的本质特性可以看到,军事信息系统的建设,不是一种普通的武器装备的研制和生产,而是需要用特殊的管理体制和建设方法来发展。军事信息系统的建设发展特色主要应该体现在其总体规划性、系统集成性、与作战指挥的密切相关性、人机结合性以及渐进获取性等方面。

### 3.1 顶层设计是军事信息系统建设的前提

系统建设要取得好的效果、要朝一体化方向迈进,一个重要的前提条件就是搞好规划和顶层设计。要实现多种系统之间的互连互通、相互兼容,确保作战信息能够在各个系统之间畅通无阻,甚至各个用户之间能够顺利进行互操作,必须从顶层设计入手进行统筹规划、制订蓝图。要根据一体化建

设的目标和要求,对系统的作战体系结构、系统体系结构和技术体系结构进行总体设计和论证。在分析各种作战需求的前提下,清楚描述系统信息流程和各种功能之间的内在联系,构建一个技术先进、成本合理、可持续发展的军事信息系统体系。

### 3.2 军事需求是军事信息系统建设的牵引

在系统的建设过程中,确定军事需求甚至比选用先进技术更重要。战术思想不明确、战法不清楚,未弄清高技术战争的基本形态,军事信息系统装备建设就会失之盲目。因此,在系统建设过程中必须坚持作战指挥理论的指导,以军事需求牵引作为第一要则。系统中指挥决策、辅助决策功能的实现都是对指挥员指挥经验、指挥艺术的归纳和提炼,军事信息系统的建设过程实际上又是一个对指挥系统的分析和优化过程,包括指挥规律的总结、指挥协调关系的整理、信息流的描述、优化模型的运用等等,是在原有的人工系统的基础上一个质的飞跃。它是信息资源的集成,更是智力资源的集成。

### 3.3 系统集成是军事信息系统建设的关键

系统集成可以分为两个层次,一个是各级各类系统本身的集成,还有一个更高层次的综合集成。综合集成是在顶层设计的指导下,通过综合整体合成、综合技术嵌入、综合扩充更新,以已建系统和已有资源特别是军事信息基础设施为基础,建立一个网络互连、信息互通、用户互操作的综合大系统。现代战争是体系与体系的对抗,那么靠什么来实现体系的对抗,靠的就是一体化的军事信息系统。即要通过系统综合集成实现各种军事信息系统之间的互联,军事信息系统与信息源、武器平台的密切交链。这很大程度上依赖于军事信息基础设施的建设,与通信资源、网络设施密切相关,因此要解决好与通信网络的建设同步协调的问题。

### 3.4 渐进获取是军事信息系统装备建设的有效途径

军事信息系统建立与其他武器装备研制的根本区别在于它有一个复杂的与应用紧密相关的软件系统,因此军事信息系统建设过程需要作战指挥参谋人员密切参与。初期研制人员与用户需求沟通会有

一定困难，即指挥人员对将要建成的这个软件系统还不能一下子明了，而系统研制人员对用户的需求也很难彻底理解清楚，同时系统的军事需求又常因各种条件和环境的变化而改变，使得开发系统时，很难一次提出十分全面、明确、详尽、定量的军事需求。往往在系统开发初期，系统应用功能可能是欠缺的、模糊的，但随着指挥人员对系统认识的深入，开发人员对使用要求的逐步明确，系统功能和目标会越来越接近用户真正的军事需求。所以军事信息系统的建立只能是渐进的，逐步完善的。在系统的组织实施过程中，还要根据作战任务的变化和战法的发展，进行功能调整或系统重组。所以国外在系统的建设中，基本上摒弃了针对常规武器系统的一次性承包法，而发展了逐步渐进法、快样法和

原型法等。同时，还要根据不断提高的需求和迅速发展的技术逐步升级，延长系统的使用寿命。

### 3.5 使用人才的素质是系统发挥效能的保证

没有一大批适应信息化建设的高素质的指挥参谋人才，就难以很好产生军事信息系统的效益。在军事信息系统建成后的组织运用过程中，要求指挥参谋人员从固有的工作习惯中解脱出来，与系统进行逐步磨合，这也是一项十分艰巨的任务。只有指挥参谋人员真正从思想观念上转变过来，提高适应信息化发展的综合素质，积极研究军事信息系统的使用和训练，最后达到能熟练地运用，才会真正提高军事信息系统装备的作战指挥效能。

### 参考文献

- [1] 刘钢，王厚生.《综合信息系统发展概论》.北京：军事科学出版社，2002
- [2] 徐洸，季福新.《现代空军指挥控制研究》.北京：蓝天出版社，2000

### 作者联系方式

通信地址：空军指挥学院训练部

邮政编码：100097

联系电话：010-66923101 010-66924115

# 军队信息化领导管理体制创新初探

符红 殷波

**摘要：**组织结构决定整体功能。随着军队建设转型的创新发展，当前的信息化领导管理体制越来越成为军队信息化建设发展的“紧箍咒”，必须加以脱胎换骨式的全面改造。本文从深入分析现行领导管理体制与信息化建设发展间存在的突出矛盾入手，提出了改革创新信息化领导管理体制的一些新举措、新思路，为切实增强部队信息化建设管理，整体推进军队信息化建设全面健康持续发展，在理论和实践上进行了初步探索。

**关键词：**军队信息化建设；编制体制；创新发展

创新是军队进步的灵魂。推进中国特色军事变革，建设信息化军队，打赢信息化战争，是全新的创造性的事业。军队信息化建设面临着前所未有的发展机遇。要整体推进军队信息化建设全面健康持续发展，唯一的出路就是，准确把握新时代的特点、高技术的发展、现代战争规律和军队建设转型等一系列重大问题，从根本上改变工业时代机械化军事思维的定势，确立信息主导、科技先行、系统集成、联合作战等新思维和新观念，顺应时代发展，大力推进建设理念、运行机制、工作行为、评估手段等建设，积极推进军队信息化领导管理体制的创新发展。

## 1 面对新发展，现行管理体制与信息化建设间的矛盾日渐突显

进入新的世纪，世界新军事变革呈现出加速发展趋势，以美国为代表的世界主要国家都致力于加强军队信息化建设，抢占新的战略制高点，谋求成为新的“霸主”。党中央、中央军委洞察国际政治风云，跟踪世界军事发展，结合我军发展实际，做出了完成“双重历史任务”的重大战略决策，提出了积极推进中国特色军事变革，建设信息化军队、打赢信息化战争的战略目标。2004年3月4日，中央军委颁发了《关于成立全军信息化领导小组的通知》，成立了全军信息化领导小组和信息化工作办公室，统一领导全军信息化工作，开启了军队信息化建设的新纪元。

根据中央军委文件精神，全军各大单位在深入研究的基础上，结合多年来信息基础设施建设，特

别是指挥自动化系统建设取得的经验和教训，相继成立了由各军兵种军政“一把手”挂帅的信息化工作领导小组，组建了信息化工作办公室和信息化专家咨询委员会，并在集团军、省军区（警备区）等团以上相关单位成立了信息化建设领导管理机构，构建了一个从军委总部、军兵种到军、师（旅）、团级相对完整的信息化领导管理体系，初步实现了军队信息化建设全面发展起始阶段中的统一组织和集中领导。

随着以信息化为核心的新军事变革蓬勃发展和军队信息化建设步伐的不断加快，现行的指挥手段和管理体制越来越突显出“实体不实、编制不全、功能不强”所带来的弊端和矛盾：体制结构“高位截瘫”，指挥关系互不顺畅，职能定位交叉重叠，管理手段简单滞后，经费保障难以为继，在相当程度上，影响和制约了信息化建设的深入发展。主要表现为，树状垂直领导管理结构纵不到底、横不到边，信息化建设“统”的力度小，宏观调控能力弱，信息壁垒和各自为阵的现象突出，信息“烟囱”得不到有效遏制，体系结构条块分割，资源使用效率低，重复建设多，信息化领导管理队伍参差不齐，各军兵种及其内部发展建设极不平衡。

## 2 采取新举措，在更高层次上推进信息化管理体制的创新发展

积极稳妥地推进信息化领导管理体制的创新发展，是适应新军事变革和军队建设转型，加速推进部队战斗力生成方式转变的客观现实要求。



2.1 适应形势定思路

思路决定出路。各级领导机关要贯彻落实好军委总部的决策指示，按照科学发展要求，认真研究，尽快确立既满足新形势新任务需要，又统一、精干、高效、有权威的信息化领导管理体制建设思路。当前，面对新军事变革加速发展的新趋势、军事斗争准备的新要求、一体化联合作战的新形势、体制编制调整改革带来的新情况，要勇于突破传统思维模式的束缚，努力实现五个转变：由指挥半机械化机械化战争向指挥信息化战争转变，由应对传统威胁向应对多种威胁转变，由粗放应急式管理导向依法分类式科学指导转变，由管理自成体系建设向组织管理综合集成转变，由指导跟进式发展向指导跨越式发展转变。总体来说，就是要坚持以新时期军事战略方针为统揽，确保部队信息化建设的强大动力和正确方向；坚持以实现信息化建设综合监管为重点，努力推动适应扁平化作战指挥需求的管理手段建设；坚持以军事斗争准备作战任务为牵引，按照打赢要求检验体制改革成效；坚持以能力素质建设为基础，着力提高筹划指导和组织协调信息化建设的能力。

2.2 抓住关节求突破

创新信息化领导管理体制是一项复杂的系统工程，必须坚持重点突破带动整体跃升。要紧紧抓住解决“腿脚”问题、解决经费问题、解决人才问题这三个关系全局性、根本性、基础性的关键环节，从根本上解决制约军队信息化建设发展的深层次矛盾和问题。

2.2.1 加强信息化建设领导机构建设

解决“腿脚”问题，就是解决目前“高位截瘫”的结构模式，充实领导力量，组建“全员满编、实实在在”的信息化领导管理机构。一是根据信息化建设的复杂性、建设任务的长期性、建设内容的高技术性和建设力量的全员性特点，在传统业务部门（如作战、情报、通信）间建立一个平行的沟通协调和统筹管理的信息化建设领导机构，实现军队信息化工作的矩阵式管理。二是在适度充实领导管理力量的基础上，按照模块化功能结构模式，细化配置，提高指挥效能。三是进一步明确职能定位，在大单位设置信息化专家咨询委员会日常工作协调联络办事机构，增强决策咨询和指导监督的能力。以军区信息化领导管理机构为例，建议调整后的矩阵式组成结构如图 1 所示。

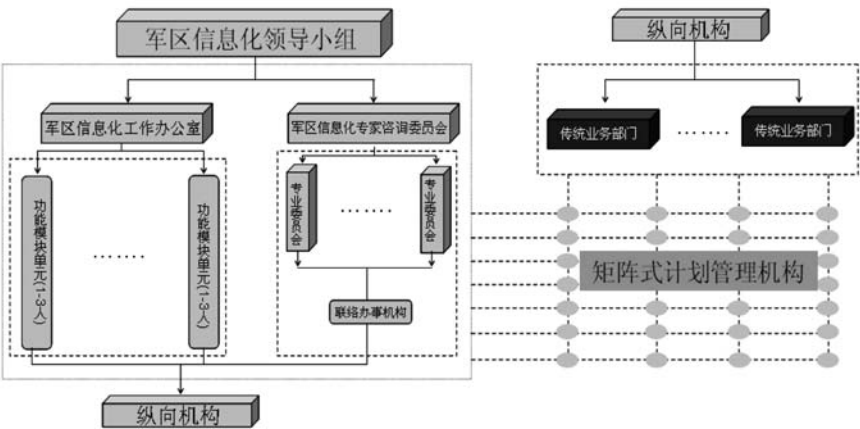


图 1 军区信息化领导管理机构矩阵式管理结构图

2.2.2 加强经费的协调与管理

解决经费问题，主要是解决各级信息化领导管理机构对传统业务部门信息化建设开展指导协调和监督管理的经费保障渠道，换句话说，就是在落实信息化领导管理机构编制实体的基础上，适度调整信息化领导管理机构的业务经费，彻底改变当前由各级通信部门支撑信息化领导管理机构开展信

息化建设统筹安排、综合评审、指导督查等工作经费的现状，规避因业务工作经费不足而引发信息化工作重复建设、各自为阵等的无序现象，确保信息化工作有统一的需求分析、统一的顶层设计、统一的建设标准、统一的协调指导和统一的推广使用，提高领导管理机构“统、管”军队信息化建设的能力。

### 2.2.3 加强信息化领导管理人才的调配

解决人才问题，就是在解决编制、经费的基础上，按照职能要求，调整领导变革型、复合指挥型和智囊参谋型人才在信息化领导管理机构中的比重。从目前的情况看，领导型、技术型、专家型和复合型领导人才在各级信息化领导管理机构中所占的比例极不协调。建议调整后的各类人才比例如图2所示。

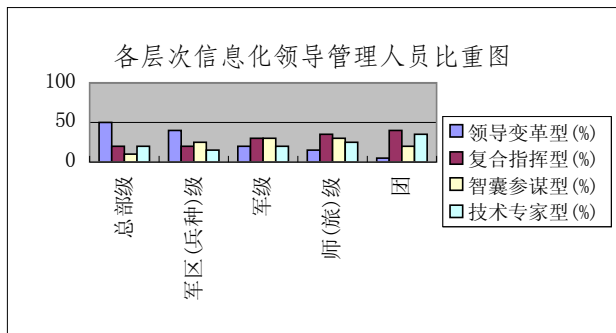


图2 各层次信息化领导管理人员比重图

### 2.3 紧贴任务抓规范

加强部队信息化建设的领导与管理是军队建设和建设转型的客观要求。紧贴职能任务规范信息化领导管理机构的工作，建立科学高效的运行机制，是履行职能、提高管理效能的重要保证。因此，各级信息化领导管理机构应在积极探索创新编制体制方法路子的同时，紧密结合职能任务和一体化联合作战的特点方法，科学划分各业务部门职能权限，明确领导和管理部队信息化建设的基本原则和基本方法，正确调整信息化建设中的各种利益关系，创新法规标准，细化、量化制度规定，研究新情况，制定新举措，解决新问题，主动作为，积极纠正工作的随意性和盲目性，努力建设信息化领导管理工作新秩序，全面开创部队信息化建设新局面。

## 3 开创新局面，推进领导管理体制变革中必须重点把握的问题

### 3.1 要把思想观念的更新放在创新编制体制工作的切入点

思想决定行动。创新军队信息化领导管理体制，不是可不可以、能不能动的问题，而是大势所

趋、刻不容缓的大事。相关职能部门要深刻认识信息化建设面临的新形势新任务，充分认清加强领导管理体制建设的极端重要性，坚持从部队建设发展的客观需要出发，坚持战斗力标准，转变思想，正确处理编制体制调整中的利益矛盾，克服贪功图全、好大喜功和知难不进、畏手畏脚的两种错误做法，坚决杜绝“假把式”，取缔“花把式”，摒弃“空把式”，紧贴实际，深入研究不同环境、不同条件下平、战时背景中的信息化领导管理体制，充分吸收军内外有益的经验 and 做法，博采众长，综合考量，具体分析，推陈出新。各级信息化领导管理机构要本着一切工作往前赶、往实里抓的思想，从难想对策，从实搞创新，求真务实，不断增强抓好体制建设的使命感和自觉性，确保编制体制调整工作落到实处。

### 3.2 要把能力素质的提高放在创新编制体制工作的着力点

能力决定作为，作为影响地位。积极稳妥地推进领导管理体制的创新，根本的出发点就是适应信息化建设发展步伐，全面提高组织领导和综合管理的能力素质，走出具有中国特色的信息化建设领导管理新路子。一是把切实增强“统”的领导管理能力放在创新编制体制的首要位置。实践反复证明，离开了强有力“统”的工作，必将导致“烟囱”林立，重复建设，资源浪费，信息化建设就是一盘散沙、一句空话，缺乏应有的生机和活力。因此，必须把是否有利于实现信息化的统一领导、统筹安排和统一协调作为衡量编制体制创新的主要标准。二是紧贴实际扎实抓好信息化领导管理机构的能力素质建设。针对不同类型的部队，不同条件的单位，从解决信息化领导管理中的“短板”、“瓶颈”问题入手，加强分类指导，加强理论研究，并结合战备演习、边防执勤、战场建设等重大军事活动，检验和改进工作指导和组织指挥方法，创造性探索新体制下多手段、高效益的领导管理模式，全面提高履职尽责能力水平。三是在军队现行编制体制的框架下努力提高信息化领导管理机构的能力素质。不管信息化领导管理体制如何创新，都离不开现行的军队编制体制框架。必须全面落实军队人才战略工程，大兴学习之风，下大力气抓好指挥军官队伍、参谋队伍、技术专家队伍的建设，为整体促进信息化领导管理机构能力素质的提高创造

良好的外部环境。

### 3.3 要把运行机制的完善放在创新编制体制工作的突破点

科学高效的运行机制，是履行职责、提高效能的重要保证。古人云，小智者治事，大智者治人，睿智者治法。要以改革信息化领导管理体制为契机，以创新和完善法规制度为途径，突出建立和完善“五种机制”：一是优化决策机制。加速信息化建设步伐，推动部队信息化建设整体发展，就是要适应未来一体化联合作战需要，建立和完善指挥控制与信息传输系统一体建设、管理、运用的决策机制。二是要建立和完善责任机制。要依据调整后的职能任务，结合各部门的实际情况，把领导和管理信息化建设的具体工作分解开来，落实到每个部

门、每个人头，努力形成各在其位、各司其职、各谋其政和齐抓共管的良好局面。三是建立健全评估机制。针对领导管理不同类型、不同级别、不同任务信息化建设的工作特点，制定和细化信息化建设检查评估标准，拿出定性和定量指标，完善领导管理绩效检查评估体系。四是不断强化协作机制。围绕信息化建设和作战需求，搞好总体设计，制定统一的工作标准法规，建立制度化、程序化的协调机制，统筹机关和部队工作。五是完善督导机制。围绕落实信息化领导小组和部队首长的决心意图，抓住信息化建设的中心工作，完善检查督办和信息反馈制度，做到扭住大事要事、盯紧责任部门、掌握工作进程、明确落实质量，扎实推进部队信息化建设整体发展。

### 参考文献

- [1] 徐小岩主编.《军队信息化概论》.北京：解放军出版社，2005.12
- [2] 戴清民著.《科学发展观与军队信息化》.北京：解放军出版社，2007.1
- [3] 吕登明主编.《信息化战争与信息化军队》.北京：解放军出版社，2005.10
- [4] 孙佳科著.《中国特色的军事变革》.北京：长征出版社，2003.12月
- [5] 姚延进，赖铭传等主编.《军事组织体制研究》.北京：国防大学出版社，1997.6
- [6] 《军队指挥自动化》杂志
- [7] 《西南军事通信》杂志
- [8] 王建民.《深刻理解中国特色军事变革战略决策，积极推进战区部队信息化建设》
- [9] 吕登明.《战区部队信息化建设对策思考》
- [10] 王晓明.《关于我军信息化创新发展问题的几点思考》

### 作者联系方式

通信地址：四川省成都市北较场成都军区司令部通信部

邮政编码：610011

联系电话：028—86681327 13880691288

# 我军信息化规划问题研究

白旭清 马献章

**摘 要：**信息化建设具有综合性、系统性、变革性、可持续性的特点和要求，迫使信息化建设在实施之前必须进行信息化规划。本文从信息化规划的概念、目标、原则、内容要素、实施方法步骤和应把握的问题几个方面，对到实践中去抓需求、抓应用，因地制宜，进行信息化规划进行了初步探索。

**关键词：**信息化建设；信息化规划

## 1 前言

“信息化规划”是一个常见的词组，出现频率很高，在谷歌（[www.google.com](http://www.google.com)）搜索引擎中达1367万条相关记录，在很多文件和报告中更是位置突出。事实上，实事求是、有特色、有远见的信息化规划确实是信息化成功的重要因素，将直接影响信息化的投入、风险、成效和进程。因此，如何实事求是地拟制定军队信息化规划的问题，就是一个极为重要的课题。

## 2 信息化规划的概念

“信息化规划”概念，来自于信息化建设所具有的综合性、系统性、变革性和可持续性的特点。信息化建设是信息化规划和信息化实施这两个层次构成的动态螺旋式递进，可大致分成以下几个环节：明确远景和使命、确立发展战略和目标、明晰军事政工后勤装备等业务及变革策略、识别关键成功因素、分析关键性能指标、抽取信息需求、建立总体信息框架。

信息化规划本质上可以定位成从业务战略到信息战略的实现。一是从发展的战略出发而不是从系统的需求出发，可以避免脱离目标而进行建设的困境；二是从业务的变革出发而不是从技术的变革出发，有利于充分利用现有的资源来满足关键需求，避免建设的信息系统无法有效地支撑作战指控、军事训练、行政管理、后勤和装备保障。

信息化规划是信息化建设的基本纲领和总体指向，是信息系统设计和实施的前提与依据，是一个

涵盖面很宽的概念。从层次上看，可分为长期规划（LP）、短期规划（SP）、信息资源规划（IRP）、信息系统规划（ISP）四个层次。这四个层次由远而近、由粗到细，逐步实现动态递进过程。

通常所说的“信息化规划”仅指信息系统规划。个别专家将信息系统规划这一层次细分为信息架构规划和信息方案规划。无论哪个层次的信息化规划，都可分解成如下环节：明确原则和任务、确立策略和目标、分析关键性能指标、抽取信息需求、建立总体信息框架。

## 3 信息化规划的核心目标

信息化规划的核心目标是引领方向、凝结共识和规避风险。

### 3.1 引领方向

引领方向是指引领作战指控、军事训练、行政管理、后勤和装备保障综合能力的提升和应用的方向。信息化规划的过程本质上是一个业务规划的过程，目标也是为了推动业务的发展，这个过程必然伴随着作战指控、军事训练、行政管理、后勤和装备保障能力的提升，而不同的发展阶段则决定了各种作战指控、军事训练、行政管理、后勤和装备保障应用方向的差别。

### 3.2 凝结共识

从管理的角度来看，一个广泛达成共识的方案要远远优于一个有创新但缺乏共识的方案。能否上

下达成广泛的共识是信息化规划方案实施的核心因素之一。信息化规划的过程就是不断梳理、明确、协商上级和下级对作战指控、军事训练、行政管理、后勤和装备保障的不同需求和看法，让信息化规划的推动者和反对者能够不断进行有效地沟通，最终获得有共识的方案。

### 3.3 规避风险

信息化规划最大的风险就是信息化建设的失败对作战指控、军事训练、行政管理、后勤和装备保障等方面所带来的严重恶果。信息化规划带来的风险主要来源于两个方面：一是规划本身不合理，选择了不合适的信息系统，使得新系统变成了“鸡肋”；二是在规划方案的执行过程中出了差错，甚至走错了方向。这些都需要事先进行统筹考虑和规划。

## 4 信息化规划的原则

### 4.1 应用需求原则

制定信息化规划必须考察应用需求，做出尽可能准确的需求分析。信息化是长期的、高投入的项目，风险较大。因此认真分析作战指控、军事训练、行政管理、后勤和装备保障的各种流程，确定恰当明确的应用需求，选择项目优先次序，是制定信息化规划的关键。

### 4.2 因地制宜原则

技术为应用服务，应用为人服务，无论先进与否，能够高效率、低成本地满足本单位、本系统需求的技术就是最适用的技术。对于信息化发展较快、信息技术较发达的部队或区域，可以适当制定较高的目标，加快信息化的进程；对信息化水平相对落后的边海防部队，不能盲目跟随，必须采取小步快进的战略。

### 4.3 近远期目标原则

规划方案具有一定的柔韧性，能适应未来一段时期作战指控、军事训练、行政管理、后勤和装备保障的变化，必须考虑解决目前存在的问题和未来发展的需求。近期目标是根据当前发展的需求和目前的

信息化技术来确定短期的目标。长远目标是通过和技术发展趋势的判断和对本单位发展趋势的分析，确定的长期建设目标。

## 5 信息化规划的要素内容

信息化规划包括一个科学的、恰如其分的目标集合，一套实现这个目标的战略路径，一系列由路径和目标规定的任务和措施。

### 5.1 信息化目标

信息化目标有时间和范围两个维度。对信息化规划的五年计划，通常可以分两个阶段，一般来说，前一阶段详细一些，后一阶段粗略一些。规划目标的定性描述要精中选精、重中选重，既要能反映全局，又要能突出重点。在目标的描述中，对定量的指标，要充分考虑数据的连续性、可比性、引导性；对定性的描述，要把本级的信息化与全军和国家发展的目标真正融合起来，从目标定位上防止不切实际的空话与大话。

### 5.2 实现信息化目标的路径

实现信息化目标的路径，通常指达到目标的实施策略、模式、过程。综合性的策略在规划中的表达方式一般包括指导思想、方针和原则，特定的策略一般体现在政策措施中。模式一般是针对一个特定的目标提出来的特定实施方法，如针对中小信息技术应用、针对普遍服务等目标的特定实施办法。过程是对切入点和关键阶段的要求，是对实现一个目标的阶段性发展描述。

### 5.3 实现信息化目标的措施

实现信息化目标的措施，也可以看做是目标的细化，任务通常倾向于反映实施中技术性和实体性的内容，措施则倾向于反映条件性、管理性、体制性的内容。分层次、分阶段的目标，通过任务措施来落实。信息化覆盖现代化全局的高度渗透性特征，决定了任务和措施的广泛性，因此，在规划中要选择具有代表性、示范和引导意义、在实施过程中不确定因素相对较少的重要内容。

## 5.4 信息化建设现状分析

认识现状,是明确起点、规划目标、决定路径的关键环节,是信息化规划中最重要的部分。现状包括成绩、经验、困难、矛盾、问题等内容,各个方面都有综合性的和专门性的两类。要理解和区分综合性和专门性,特别是要在许多专门性的现状中找出综合性的内涵。要进行深入的调查研究,要充分利用各类现有的资料,要把总量(整体)和典型结合起来,以得出科学的结论;要把握事物的本质,防止分析的表面化,把一时一事一地的局部性经验或教训误认为是全局性的;要防止片面性,纵览全局、进行深度分析;要恰当区分困难、矛盾和问题,才能有的放矢,提出有针对性的解决办法。分析现状,要十分注意总结和归纳,科学地梳理错综复杂的现象,分门别类,找出规律,而不是罗列现象,或者是不恰当的归纳和综合。

## 5.5 信息化建设的发展趋势分析

分析和把握趋势是做好信息化规划的关键环节。把握趋势与分析现状有相似之处,主要的不同在于把握趋势更加依赖历史数据,通过对历史和现状的分析,判断未来的走向。在对趋势的把握中,尤其要注意技术的发展趋势,因为技术革命是网络和应用发展的基础。

## 5.6 信息化建设的需求

决定信息化发展方向和力度的是需求和预期效果,是作战指挥、军事训练、政治工作、后勤和装备保障等各个方面的需求和预期效果。信息化规划与军事发展规划结合的基础就在于对需求的分析,必须正确把握并从本质上理解诸军兵种的作战、训练、管理、保障等内容,分析和归纳总结出信息化建设的关键和重点。

## 5.7 信息化建设的条件

确定发展目标和实施路径,不仅要分析需求、现状和趋势,还要正确把握基础条件,尤其是指出关键的制约因素。一是全军发展的整体水平,二是本级的人才基础,三是全军和本级的实践基础,四是本级和所属部(分)队的体制。此外,还有很多基础条件需要在编制规划时重视(如资金、技术、

安全性等),需要在编制的过程中,要在给予充分分析的基础上得出结论。

## 5.8 信息化规划的操作性

操作性是一个比可行性更复杂、缺乏固定内涵或外延的名词,有具体的数字、具体的工程、具体的目标不。强调可操作性不等于失去宏观性,宏观指导、全局部署是中长期规划的内在要求,不等于不要定性描述的目标和任务,不等于不存在一些远期目标和任务的模糊性。可操作性来源于扎实的基础工作,主要是基于前面关于现状、趋势、需求、基础条件等方面的讨论。

# 6 信息化规划的方法

军队信息化是一项持续的工程,信息化规划多为中长期的,需要在规划实施期间对规划内容做出持续改进和完善。通常包括以下几个过程。

## 6.1 环境分析

对本级所处的环境进行分析是信息化规划必不可少的工作,它是规划的依据。需要深入分析本级所处的军兵种和地域宏观环境以及具有的优势与劣势、面临的发展机遇与威胁等,如西藏地区和内地应有很大的不同。

## 6.2 战略分析

本级信息化是为本级战略目标实现服务的。要明确本级的发展目标、发展战略和发展需求。要明确为了实现本级的总目标,各个关键部门要做的工作,要理解本级发展战略在编制体制结构等方面的定位。在此基础上,通过分析,明确上述各个要素与信息技术特点之间的潜在关系,从而确定信息技术的驱动因素,使信息化与本级战略实现融合。

## 6.3 分析与评估现状

对本级的现状分析与评估应该从两个方面着手:本级的业务能力现状和IT能力及现状。业务能力分析是对作战指挥、军事训练、政治工作、后勤和装备保障业务与管理活动的特征、各项业务活

动的作业模式、业务活动对战略目标实现的作用进行分析,揭示现状与远景之间的差距,确定关键问题,探讨改进方法。信息化现状分析是诊断本级信息化的当前状况,包括基础网络、数据库、应用系统状况,分析信息系统对未来发展的适应能力,给出信息化能力评估。

## 6.4 关键业务流程分析与优化

在前三步的基础上,分析并确定那些流程中不合理、效率低、与战略目标不符的流程及环节,发现能够在现有环境中实现战略目标,并使提高战斗力的关键驱动力以及关键流程,从而根据战略目标和外部环境,进一步优化流程,实现信息化与业务上的融合。

## 6.5 信息化需求分析

需求分析是在战略分析和现状评估的基础上,按照优化流程的业务运作模式,制定适应未来发展的信息化战略,指出信息化的需求。需求分析包括系统基础网络平台、应用系统、信息安全、数据库等需求。

## 6.6 信息化战略的制定

包括三个方面的工作:一是根据本级战略需求,明确信息化的远景和使命,定义信息化的发展方向和信息化在实现战略过程中应起的作用;二是起草信息化基本原则,它是指为加强信息化能力而提出的基本的准则和指导性的方针,是有效完成信息化使命的保证;三是制定信息化目标,它是在未来几年为了实现远景和使命而要完成的各项任务。对于所形成的每一个业务构想,明确 IT 对其支持的理想状态,即 IT 战略目标。

## 6.7 确定信息化的总体构架和标准

在发展战略目标的指导下,基于业务发展需求和对信息化的需求,首先,从系统功能、信息架构和系统体系三方面对信息系统应用进行规划,确定信息化体系结构的总体架构。同时,还需要拟定信息技术标准。这一部分涉及到对具体技术产品,技术方法,和技术流程的采用。它是对信息化总体架构的技术支持。通过选择具有国标、国军标甚至应用最为广泛、发展最有前景的行业标准,可以使信

息化具有良好的可靠性、兼容性、扩展性、灵活性、协调性和一致性。从而提供安全、先进、高效的服务,并且降低开发成本和时间。

## 6.8 信息化项目分解

将整个信息化过程分解成为相互关联,互相支撑的若干子项目,定义每一个项目的范围、业务前提、收益、优先次序、以及预计的时间、成本和资源;并对项目进行分派和管理,选择每一项目的实施部门或小组,确定对每一项目进行监控与管理的原则、过程和手段。

## 6.9 信息化保障分析

针对每个项目,进行保障性分析,即按重要性排列优先顺序,进行准备度评分,并根据结果做出初步取舍,形成路标规划。然后对项目进行财力分析,根据总部任务和本级可能的自筹资金的能力,决定取舍。

# 7 信息化规划应把握的几个问题

## 7.1 长远规划与适应变化之间的平衡问题

在信息化规划的过程中,最突出的问题是既要尽可能地保持开放性和长远性,以确保系统的稳定和延续性;又要因为规划没有变化快,需适时对规划进行相应地修改。这一问题目前还没有非常理想的解决方法。相对有效的做法是,在进行信息化规划时,认真分析本级信息化建设与信息技术支撑之间的影响度,并合理预测军事发展变化可能给规划带来的偏移,在规划时适当留有余地,做务实的牵引,不要追求大而全。

## 7.2 传统工作流程与软件系统流程之间的平衡问题

传统的作战指控、军事训练、行政管理、后勤和装备保障工作流程与作战编组、编制体制结构是由传统的技术所决定的。反过来,采用新的信息技术和信息系统也必将影响着其作战指控、军事训练、行政管理、后勤和装备保障工作流程和作战编组结构。到底应该是改变传统工作流程来适应软件,还是修改软件来适应传统工作流程,这个并不



重要，重要的是如何有效利用信息技术大大提升部队的战斗力。要着眼长期的发展，战斗力的提高，改变人们的思维方式，让工作流程去应软件系统。

### 7.3 管理变革与技术变革之间的平衡问题

诸军兵种以及各作战集团、作战部队、作战分队的变革需求往往是信息化建设的一个重要原因。比如，在全军一体化训练试点中，出于提高指挥效能的考虑，必须将纵长横窄的指挥体制变为纵短横宽的扁平式指挥体制。技术的变革同样是迫切和必要的，从单主机应用到客户机/服务器应用，到浏览器/服务器应用，再到客户机/服务器与浏览器/服务器混合应用，每一次技术的演进都能带来作战指挥、军事训练、行政管理、后勤和装备保障的巨大变革和更大的想象空间。不过，这在不同的单位，是有不同的需求（比如院校、科研机构和作战部队、后勤装备保障单位以及作战指挥各要素等），不同的变革需求必须有不同的解决方案特别是不同的技术方案去满足。

### 7.4 信息化规划各层级之间的平衡问题

在信息化规划中的信息战略、信息资源、信息系统、单位资源规划这四个层次之间，同样应该有一个很好的平衡。完整的信息化规划，无疑应具备上述的四个层次，而且理想的规划应该是分层递进

参考文献（略）

#### 作者联系方式

通信地址：四川省成都市北较场成都军区司令部通信部

邮政编码：610011

联系电话：028-86681332 86681328

的。比如信息化基础差的单位在推进信息化时，就可能有多种选择，比如：不经过信息资源规划，直接进行信息系统规划；或者不经过资源规划，就选择最急需的、又容易实施的模块（如训练管理、办公自动化、信息检索与支持、装备器材管理、经费管理等）先上，待见成效后再回头做战场感知、情报处理、作战计划（方案）辅助生成、作战能力评估、面向作战指挥的精确信息保障服务等。

### 7.5 信息化规划与建设实施之间的平衡问题

信息化规划的目的是为信息化建设和实施提供框架指南。事实上，这二者之间存在天然的断层。原因主要出自于不同的参与者所站的立场不同。在信息化规划阶段，通常应该是由各级信息化办公室牵头，信息化专家咨询委员会参与，作战、情报、通信、国防动员、政治工作、后勤保障和装备保障等业务主管部门积极配合；而在信息化建设实施阶段，则以作战、情报、通信、国防动员、政治工作、后勤保障和装备保障等业务部门主导、其他业务部门配合。如何确保信息化规划在后期的实施建设过程中不走样，单纯靠业务主管部门去协调和监督，效果是不会理想的。最好的解决办法是，发挥专家咨询委员会的职能作用，推动和监控信息化建设实施过程，确保信息化建设实施的无缝衔接。



# 努力适应应用主导的客观要求 积极推进军队信息化建设全面协调发展

张云水

**摘要：**在我军信息化建设全面发展的起始阶段，正确地认识和把握应用主导规律是促进我军信息化建设健康、有序发展的关键环节和重要保证。只有正确地遵循应用主导规律，才能能够正确认识信息化发展的客观规律，及时发现和正确解决各种问题和矛盾，不断修正发展方向，实现真正意义上的信息化建设全面协调发展。

**关键词：**应用主导；军队信息化；军队建设；协调发展

军委把我军信息化建设定位于全面发展的起始阶段，这一判断既符合信息化发展的一般规律，也符合我军信息化建设的实际水平。在当前我军信息化建设跨领域全面发展即将启动的重要时刻，必须深刻认识我军信息化建设现阶段特征，努力适应应用主导规律，紧紧抓住信息系统网络的应用牵动功能，逐步实施跨领域综合集成建设，积极推进我军信息化建设全面协调发展。

## 1 适应应用主导规律是我军当前信息化建设的迫切要求

信息化建设是一项系统工程，处理好当前与长远、局部与全局、重点与一般的关系，找准切入点，是赢得主动权的关键。我军指挥自动化建设的历程，国家信息化建设的发展，外军信息化建设的经验，无不启示我们，立足当前信息化建设的现实，主动适应信息化发展应用主导规律，突出系统应用，是确保我军信息化建设全面协调发展的必然选择。

### 1.1 从我军指挥自动化建设的经验教训看，应用主导是信息化建设的重要保证

当前，我军指挥自动化建设存在问题的主要原因是对应用主导的规律认识和把握不够，各级不同程度地存在“重建设、轻使用，重硬件、轻软件，重开发、轻数据”的问题。总结 20 年的经验和教训，主动适应应用主导规律，从建设、使用、管理的全过程落实应用主导，实现建用互动，是提高信

息化建设效益，促进信息化建设协调发展的重要保证。

### 1.2 从国家信息化建设的发展进程看，应用主导是信息化发展的必然选择

国家信息化从 1993 年正式启动以来，借助国家经济发展的强大动力，建设水平不断提升，目前已进入全面发展阶段，国家推进信息化的一条重要经验和基本举措，就是着眼经济发展和社会进步，始终以应用需求为主导，注重信息技术在国民经济和社会生活中的渗透应用。由于有商业推动这一巨大的动力，建设者及时检验效益、努力改进系统，使用者不断提出需求、丰富系统功能，国家信息化建设在应用上取得了显著成效。即便如此，国家信息化建设主管部门和权威专家在总结经验教训时，把“信息化效益不够明显，应用落后于建设，资源利用落后于开发”作为主要问题之一，指出“信息化发展未能与实际需求形成良好互动，需求与应用结合不够是信息化发展缓慢的主要原因”。由此可以看出，应用主导既是信息化建设的重要原则，也是信息化发展的基本规律。

### 1.3 从我军信息化建设的发展现状看，应用主导是信息化建设的迫切要求

我军信息化建设正式启动虽然只有几年的时间，由于有军委首长的亲自领导和各级领导的高度重视，发展进步比较明显，但也存在一些亟待解决的问题，主要表现在：思想观念落后，没有形成信

息化的体系融合观念；一体化设计薄弱，缺乏清晰明确的发展战略和军队信息化体系结构；缺乏实时高效、横向联合的应用管理体制，条块分割式管理，造成部门利益意识突出，受局部利益驱使，自成体系，相互封闭，难以在实际运行中统一起来；系统建设缺乏应用检验和评价，使建设项目科学批判不够，证实与证伪不足。上述问题的存在，原因是多方面的，从部队信息化建设实践的角度认真反思，没有实现统一平台下的一体化应用是主要原因。军队信息化建设包括信息网络、信息系统、信息资源、信息人才等诸多方面，信息系统建设是信息化军队赖以生存和发展的物质基础，没有高度发达的信息系统作支撑和牵动，军队信息化建设就难以协调发展。信息系统建设成败的关键在于在实际运用，对此，全军上下需求迫切。当前，之所以各自开展建设，既是军事斗争准备对信息系统的应用需求，也是当前部队分领域独立建设向跨领域全面发展过渡期，运用网络应用牵动功能促信息化建设协调发展的科学选择。集中反映了全军部队对应用主导的渴望与需求。在统一的应用模式下实现系统集成，构建全军统一的指挥平台，在应用中促动深化，在应用中牵动全面发展，促动战斗力生成模式的转变，已成为当前信息化建设的迫切需求。

#### 1.4 从外军信息化建设的发展过程看，应用主导是信息化建设的基本规律

军队信息化建设走在世界前列的西方主要国家，无不把应用主导作为抓信息化的基本规律来把握，美军在总结信息化建设初期的经验教训的基础上，走出了一条“先大后小，先总体后局部”的路子，把主要精力放在了综合信息系统建设和应用上，在基本确保综合信息系统的高水平发展之后，才真正开始解决各局部信息系统的连接问题。从我军引进的指挥自动化系统来看，其硬件水平低于我军的同类装备，但软件水平、集成水平、应用水平远远超过我军的相应系统。分析其原因，主要是坚持了应用效益这一根本标准，从需求论证、系统研制、操作使用，无不做到了实用、好用、管用。目前，世界各国特别是西方发达国家在军队军事系统应用的主要做法是虚拟实践，其本质就是运用计算机、网络和虚拟现实等信息技术手段，创造一种模拟未来战争的“人工合成环境”，让军人在这种网络空间和电子空间构成的虚拟环境中进行“预实

践”。显而易见，虚拟实践是未来平台整体运用、全面检验、逐步提高的过程，是对应用主导规律的深入实践，是实现系统集成、建用互动、以用促建的有效途径。

## 2 遵循应用主导规律，抓好信息化建设的主要任务

认识规律，把握规律，遵循规律，是科学发展观的内在要求。当前我军信息化建设的关键，是抓好军队指挥信息系统的建设和应用，重点要做好系统集成、资源开发、虚拟实践、人才培养等工作。

### 2.1 要抓系统集成

系统集成是把很多军事系统集成成一个大的军事系统，要用大系统的观点来统揽信息化建设的方方面面，以不断提升军队的信息化程度和一体化水平。对各部门、各系统分立自建的侦察监控、网上办公、装备保障、物资管理等信息系统进行一体化改造，形成统一的应用模式和标准体系，在建用互动中逐步解决分立建设、重复投资的问题，为实现信息系统系统集成奠定基础，以此逐步推进未来平台的发展提高。

### 2.2 要抓资源开发

军队信息化建设仍处在系统建设为主的阶段，要积极汲取国家信息化建设的经验教训，在信息系统建设过程中，同步规划信息资源开发利用工作。一要“死库”变活。从机关做起，对各部门在用数据库系统进行一次全面普查，搞清楚现有数据库系统的数量、用途、使用范围、技术状况等，运用最新网络融合技术，实现单机系统向网络系统的改造。二要“活库”联合。按照统一的数据格式，以指挥自动化三期网为依托，以有效的安全保密体系为保障，将各部门、各系统独立使用的系统从单一用户、部门权益中解放出来，实现这些数据资源按权限向首长和特定用户的共享，逐步形成网络使用模式。三要资源融合。按照统一的建设标准，以平台为基础，建立完善军区作战指挥、情报侦察、电子对抗、军事训练、安全管理、国防动员等专用信息库，力求形成面向不同主题、通联各个部门、动态更新的战役战术综合数据库系统。

## 2.3 要抓虚拟实践

未来战争先胜于实验室、实验场，后胜于战场的特征越来越突出，虚拟实践已成为一条重要途径，西方发达国家军队无不把虚拟实践作为信息化建设的一项重要任务。我军要实现跨越式发展，就必须从现在做起，大力开展虚拟实践研究和建设工作。一是要在战略决策部署上重视虚拟实践工作。要把虚拟实践作为推进信息化建设、检验军事斗争准备水平、提升信息化实用水平的重要举措，从顶层设计、全局规划上搞好部署、抓好落实。要借助战略、战役演习等大型军事活动，结合实战准备，有计划、有步骤地积极推进。二是要在信息技术研究上重视虚拟实践工作。要发挥我军信息化建设的后发优势，依托军地有关院校、研究所，加大军事运筹、模拟仿真、图像识别等技术的研究运用，力争形成我军自主知识产权的虚拟实践技术体系。三是要在开展军事训练上重视虚拟实践工作。要按照未来战争的发展趋势，在军事训练中大力开展信息化练兵活动，在虚拟作战条件和战场环境中，检验信息化武器装备，提高作战人员的实际能力，锻造指挥人员的组织指挥能力。通过这种‘预实践’对军队信息化建设项目和成果，进行实验、检验、评估、论证或完善，得出有关数据和结论，用于指导今后的信息化建设。

## 2.4 要抓人才培养

把握信息化人才生成规律，牢固树立人才先行的观念，超前培养、开放培养、跨越培养，发挥后发优势，努力提高人才培养的质量。要按照提高打赢联合作战能力的要求，打破军兵种界限，联合培养复合式信息人才群体；要发挥院校人才培养的主阵地作用，建立完善的信息化学科体系，调整专业设置，打牢信息化人才培养的基础；要按照未来战争需求，建立信息化平台，创造良好的虚拟实践条件，培养满足实战需求的信息化人才；要围绕信息系统的的核心需求培养人，使决策者、使用者、开发者能围绕平台建设用中育人，不断提高人员的信息素养和信息意识，实现人员积极性和系统可用性的良性互动。

## 3 对策建议

### 3.1 转变观念、统一认识，确立应用主导的建设理念

全军上下高度重视信息化建设，但在基本观念和操作层面上存在一定的分歧，特别是对应用主导这一基本规律的认识和把握还很不到位。为此，要建立形象生动的信息化建设和信息化战争模型，认清信息化建设的网络化特征，奠定以网统建的思维基点；认清信息化建设的系统性特征，确立“平台”抓手促整体联动的实践基点；认清科学发展观的人本原理，选准建立评估机制促潜能挖掘的动力基点。要以军事斗争准备为牵引，以“网统”理念为指导，以平台建设为抓手，以系统集成途径，以质量评估为推动，以用促建，建用互动，以应用促网系融合，以应用促资源整合，以应用促人才培养，以应用促资金聚合，以用促信息化建设全面协调发展，以应用推动战斗力生成模式的转变。以此统一抓建的思路，明确建设的途经和步骤，奠定应用主导的思想基础，赢得信息化建设指导的主动权。

### 3.2 突出重点、典型引路，创立应用主导的激励机制

在我军信息化建设全面发展的起始阶段，各系统的分工建设任务仍很艰巨，既要按整体筹划抓好建设，也要发挥各系统、各部门的主观能动性，创造性的完成任务。要制定政策，营造氛围，在充分运用已有条令条例、法规性文件的基础上，针对信息化建设需要，制定出台一系列切实可行的奖惩制度；要区分优劣，透明势差，把信息化作为部队党委、机关抓大事、谋大事、务大事的重要内容，作为检验一级党委班子政绩和主官素质的重要指标，作为评定单位军事斗争准备质量高低的重要尺度。通过透明政绩势差，克服信息化建设中的盲目乐观、自以为是现象，增强紧迫感和使命感；要功过严明，奖惩导向，注重挖掘和培养关键领域、重点方向、重点系统的典型单位和个人，切实把信息化建设实绩与个人切身利益紧密挂钩，宣扬和重奖工作成绩突出者，对违背规律，导致决策失误的领导，要在行政上给予追究，通过奖惩引导信息化建设健康发展。

### 3.3 着眼发展、深化细化，建立应用主导的法规标准

法规制度是一切建设走上规范化、制度化、长效化的基本保证，信息化建设覆盖范围广、涉及部门多，必须建立一套科学、实用、可操作性强的政策法规。要采取“废、改、立”相结合的方法，自上而下地对现行的政策法规、制度规定，进行重新审视和系统梳理，着眼信息化建设中不断出现新情况和新问题，废除那些不合时宜的内容，充实完善那些不够到位的地方，及时出台一些新的制度规定，尽快构建针对性、操作性、系统性强的法规体

系，指导和规范各方面的建设行为，使信息化建设有法可依、有章可循。技术标准是确保信息系统和信息资源开发一体化发展的基础，要以我军指挥自动化建设积累的标准规范和实践经验为基础，按照稳定性与灵敏性相结合、前瞻性与现实性相结合的原则，着眼一体化建设需求，及时进行充实、完善，细化信息化建设的具体技术标准，形成信息获取、交换、发布、使用等方面的技术标准体系，确保新建系统无缝互联、互通、互操作，已建系统有一体化的改造标准，为逐步实现系统集成奠定基础。

#### 参考文献（略）

#### 作者联系方式

通信地址：兰州军区司令部通信部

邮政编码：730000

联系电话：0931-8981192

# 浅析信息化条件下体系破击作战指挥应具备的几种能力

李广文 李汉琛

**摘要：**体系破击战是一体化联合作战的基本作战样式。提出了并分析了信息化条件下体系破击作战应具备的 5 种能力：实时准确获取情报信息的能力、科学高效做出指挥决策的能力、缜密精确制定作战计划的能力、精确实施远程协调控制的能力、确保指挥系统足够生存的能力。

**关键词：**体系破击战；作战指挥；能力

信息化条件下的体系破击作战，是以信息技术的高度发展、军队信息化程度的提高为基础而产生的一种全新的作战方式。综观世界范围内近期发生的几场具有体系破击作战特征的局部战争可以看出，体系破击作战指挥应具有以下几种能力。

## 1 实时准确获取情报信息的能力

体系破击作战中，能否获得实时、精确的情报，不仅是指挥员和指挥机关实施作战指挥的前提和保证，而且也是衡量有无条件组织实施体系破击作战的首要标准。近期几场局部战争中，美军之所以能够有效运用体系破击作战方式，一个重要的原因就是拥有相对完善的情报、侦察、监视系统，可以近实时获取准确的战场信息，全维感知敌方活动，从而掌握作战的主动权。

### 1.1 精选打击目标的要求

精选打击目标是体系破击作战的第一步，也是较为重要的一个环节，它的实施好坏对后期作战有十分重要的影响。所谓精选打击目标，就是要通过侦察情报，对敌作战体系进行全面的研究、分析，找出敌体系之重心，正确选择敌体系的要点目标。这个过程依赖于实时准确的情报信息，如果没有供指挥员使用的实时准确的情报信息，对敌作战部署模糊不清，就把握不住作战重心，找不出作战关键点，体系破击作战中的精选打击目标也只是无稽之谈。

### 1.2 实现精确打击的要求

现代高技术条件下的体系破击作战，要实现精确打击，关键就在于战场透明，在于情报获取的精确性上。也就是从目标的发现、识别、跟踪和锁定，到武器的制导及毁伤效果评估等，都需要精确的情报保障，只有实现了精确侦察、精确定位、精确控制、精确评估手段，才能使精确打击成为现实，使影响指挥员做出正确决策的“战争迷雾”得到消除。科索沃战争之前，北约已开始动用多种手段对南联盟进行侦察监视，对主要目标进行了精确测量和定位。作战中，美国利用部署的 24 颗 GPS 全球定位系统卫星，北约利用 50 多颗军用和民用卫星，为多国部队提供情报服务，从而有力地保障了远程精确打击的准确。

## 2 科学高效做出指挥决策的能力

体系破击作战中，作战进程和节奏明显加快，战场情况变化急剧，必须强调指挥决策的科学性和高效性。信息化条件下体系破击作战，一方面，由于信息化战场上微电子技术、计算机技术、激光等新型作战手段的运用，信息的传递速度接近光速，导致信息的获取、传输与处理显著加快，指挥周期即从获取信息到采取行动的时间过程大大缩短。另一方面，信息化武器系统、多样化的作战平台、C<sup>4</sup>ISR 系统的建立与完善、软硬结合的电子战装备、新型的夜视器材的大量使用，从根本上改变了整个作战的运动速度和运行状态，从而使时间特性发生重大变化，导致单位时间内的作战效能显著

增强。再一方面,对抗空间的多维性、对抗力量的多元性、对抗手段的高技术性和对抗行动的整体性,使敌对双方对有效时间和空间的争夺范围更广,程度更为激烈。海湾战争中,美军在开战之前实施的“白雪行动”,仅以5小时的高强度电子攻击,就使伊军苦心经营多年,由先进的苏制导弹、高炮所组成的防空体系瘫痪,多数指挥系统失灵,为美军空中作战开辟了通路。最后,战争目的的有限性和作战的高效率,使作战的坚决性和速决性更加突出。高速度、全纵深、全领域、全时空、全频谱不停顿对抗行动,使得对抗双方在作战过程中更加强调把握战机。在作战指导上,交战双方都力求以快制敌,在对方未做出有效反应之前即采取新的行动,使对方应接不暇,在最短的时间内结束战争。所有这些,都导致战场情况变化急剧,节奏明显加快,优劣态势转换频繁。因此,对作战指挥决策的科学性和高效性提出了更高的要求。战场上的分秒失误,都可能被敌方利用,由于战场态势、作战部署、作战行动和有利战机的出现具有瞬息万变、短促急剧的特性,因而时间差、速度差、信息差都将对作战结局起决定性的影响。

### 3 缜密精确制定作战计划的能力

体系破击作战的主要作战手段是使用精确制导武器进行精确打击,其目的是在适当的时机、适当的地点,以远程精确火力摧毁或瘫痪对方的重要目标。要实现这一目的,作战计划就必须全面、周密,在目标选择、力量使用、持续时间和作战行动评估等一系列环节上进行周密的筹划。

#### 3.1 体系破击作战中精确打击依赖精确计划

体系破击作战中,打击目标由以往的地区目标、概略面状或片状目标向点状目标、精确目标转化。要实施精确打击,就必须选准作战目标,合理分配作战力量,周密组织计划,以求一击制敌。体系破击作战的组织计划必须注重作战效果,提高计划精度,改变过去那种“不惜一切代价”的“粗放”式估算模式,提高组织计划的精确性。

#### 3.2 参战力量多元要求计划更加精确

体系破击作战,是诸军兵种共同实施的联合作

战,而且局部战争作战目标和目的有限,作战节奏快,时间短。在较短的作战时间、相对狭小的作战空间内,各军兵种需要根据各自武器优长,从相距几十千米、几百千米甚至几千千米的位置和发射阵地,同时集中火力,以达成统一的作战目的。如不事先制定精确的作战计划,作战效果就会“事倍功半”,就可能无法实现作战目的,甚至有可能出现自己打自己的“误击”。这同样要求体系破击作战中的组织计划必须精确、周密。

## 4 精确实施远程协调控制的能力

体系破击作战中,战场空间广阔,情况变化急剧,对指挥控制能力提出了更高的要求。精确控制作战空间、打击目标、作战时间和作战效果,已成为体系破击作战指挥的重要特征。

### 4.1 作战空间控制要求更加精确

体系破击作战,战场涉及多维立体空间,既有传统的陆、海、空三维空间的交战,又有太空、电磁、网络等全新领域的对抗。各个作战空间既相对独立又相互交叉重叠,单维对抗被多维对抗所代替。作战控制必须着眼于整个作战空间,而不能只注重单维空间内的具体作战行动。同时,精确制导武器和远程火力的大量运用,要求对作战空间进行科学合理的划分,实现对作战空间的精确控制。

### 4.2 作战时间控制要求更加精确

作战时间控制是以时间为具体控制标准,通过对作战行动的时间安排来掌握作战行动的进程,从而控制所属各部队作战行动的一种控制方法。在参战军兵种多、作战节奏快的情况下精确控制行动时间,不仅可以减少战场混乱,而且可以提高作战效能。体系破击作战中,对时间协同的准确性提出了近乎苛刻的要求。如在美军打击利比亚的“黄金峡谷”行动中,美军三批参战飞机分别从位于英国的三个空军基地起飞,在夜幕中保持无线电静默飞行5000余公里,到达地中海上空,与从航空母舰上起飞的海军舰载机在攻击阵位上集结,时间相差仅数秒。这种诸军兵种间高精度的时间控制与协同,是“黄金峡谷”行动取得成功的关键。

### 4.3 作战目标控制要求更加精确

未来体系破击作战,作战目标有限,作战规模和力量使用受到政治、经济和外交等因素的制约,强调选择对战争进程有重大影响的目标予以精确打击。要精心侦察并选择、确定敌方的重要目标,有效利用打击手段,不使战争升级、规模扩大。对选择的作战目标,是全部打击还是局部打击,是同时打击还是依次打击,是警告性打击还是毁灭性打击,都要严格控制,实施精确的打击。美军制定的“五环”目标选择理论,就是美军确定打击重心的主要指导原则。作战目标选择上的严格要求,使体系破击作战指挥中作战控制活动的精确化趋势日渐明显。

### 4.4 作战效果控制要求更加精确

体系破击火力打击,在确定打击目标后,对打击的程度和效果要制定严格的量化指标。如在伊拉克战争中,美军对信息作战的打击强度作出严格的规定。在战争初期,并没有像以往那样对敌方军事和民用信息系统发起大规模信息进攻,只是有选择地对伊指挥信息系统、通信和防空信息系统进行了干扰、压制。精确控制作战效果,已成为信息化条件下体系破击作战指挥控制的重要内容。

## 5 确保指挥系统足够生存的能力

未来信息化战场,指挥系统生存环境的安全系

数呈现出急剧下降的趋势,指挥系统日益成为敌对双方以软硬手段综合打击的首选目标。指挥系统一旦被摧毁,整个作战行动将处于瘫痪状态。美军“空地一体作战理论”就明确提出,现代战争“打击和歼灭敌人后方目标是不必要的,应最优先打击敌方的指挥控制系统”。随着高新技术的不断发展,已经为这种作战理论付诸实践提供了必要的物质条件。如利用部署在全维空间的电子、成像、光学、监听、测向、定位、遥感等技术侦察设备,可以准确无误地发现、识别对方各级作战指挥机构的性质和具体位置;使用各种打击距离远、信息化、智能化程度高、摧毁力强的精确制导弹药,可以直接准确地攻击和破坏对方深远纵深内的坚固工事;综合运用信息化作战平台、精确战、点穴战、瘫痪战、电子战等新的作战样式,硬杀伤能力大大提高,“发现即摧毁”将不再是神话。近期几场局部战争中,美军就反复上演了“斩首”、“震慑”和“点穴”战。沃登提出的以领导指挥层为中心环的“五环模型”理论,也被美军有关条令所吸纳。敌军也高度重视对我指挥控制系统的打击,如其先制反制突击,将在我第一波联合火力打击前1小时或同时或“第二击”发起前夕,运用占总数10%~20%的战机空中突袭、陆军部分地地导弹部队和10%~15%的海军作战舰艇导弹攻击、外岛压制性火炮打击以及三军特种部队破袭等手段,重点对我浅近纵深地区的机场、港口、炮导阵地、指挥所、雷达技侦阵地、交通枢纽等目标,尤以重要军政设施为“第一优先”。

### 参考文献

- [1] 杨东辉等.体系破击作战指导四则.军事学术,2006.11
- [2] 于学亨.实施体系破击与建立完善的作战体系.国防大学学报,2006.6
- [3] 赵宗歧.信息化作战指挥研究.北京:军事科学出版社,2005.1

### 作者联系方式

通信地址:济南市经十一路80号通信部信息化工作办公室

邮政编码:250002

联系电话:0531-51685630

# 基于电子军务的我军首席信息官制度建设初探

李振富 吴垚 李旭东 史雅宁

**摘要:** 从企业的电子商务、政府的电子政务和我军信息化建设的发展中,提出电子军务时代的到来。而信息官制度伴随着电子商务和电子政务的发展而诞生,并在美军中得到普及,成为了电子军务时代我军编制体制改革的一个重要着眼点。通过仔细分析我军现行信息组织管理体制中存在的一系列问题,提出有必要在我军成立信息官制度并意义重大。最后,给出了我军信息官制度的总体框架和各岗位职能,并提出了几个应该注意的问题。

**关键词:** 电子军务; CIO; 信息官制度; CIO 团队

信息化建设是我军积极推进中国特色军事变革,打赢信息化战争的必由之路。经过 20 多年的艰苦努力,我军信息化建设已经初步取得了显著的成效,但是在建设的过程中暴露出顶层设计不够、超前意识不强、信息共享困难、办事效益低下等问题。随着军务活动逐渐实现无纸化,网络化,各种基于网络的应用系统越来越多,电子军务在我军逐渐得到普及,上述问题对我军的信息化建设的困扰显得越来越严重。借鉴国外和地方信息化建设经验,建立我军信息官制度,对我军信息化建设的组织领导,促进我军信息化建设的快速、持续、健康、协调发展具有重要的理论和现实意义。

## 1 电子军务和首席信息官制度

### 1.1 电子军务

“电子军务”是我军著名信息安全专家、中国工程院院士沈昌祥提出的。由于电子军务发展时间较短,运行中还处于摸索阶段,所以对它的定义众说纷纭。2001 年有人说:电子军务是指利用以数字化通信为核心的信息技术,从事军品生产与采购、武器装备维护与管理、高新技术武器研制与生产等一系列军品和技术交易的活动。2004 年有人说:电子军务,简单而言就是军务工作电子化,即指应用计算机网络技术和管理理论,对我军各种传统军务(如军队行政管理、装备管理与采购、后备动员管理、人力资源管理、各级党委党务工作及思想政治工作等)进行持续不断的革新和改善,以实现高效率的军队管理。2007 年有人说:电子军务

是一种综合体系,它囊括了信息环境下军事领域的方方面面,既包括了国防管理的范畴,也涵盖了军队管理的领域,日常内部军事管理、装备采办管理、训练管理、数字化军队管理、数字化战场管理。具有指挥、控制、情报、监视、侦察、反情报、导航定位、公共信息管理和信息战等功能。

可以看出,我军对电子军务的定义逐步向指挥自动化和战场环境转变,这是继企业的电子商务和政府的电子政务后在军队内发起的以计算机网络为基础的信息化革命。我们的理解是:对各种军事信息资源进行合理的管理和规划已经进入到以计算机信息网络等作为载体的这样一个阶段。美军从上世纪九十年代就开始就着手 C<sup>4</sup>ISR 的建设,这是电子军务发展的较高阶段,并且成立了与之相关的组织管理体制:首席信息官制度,用来管理美军的信息化建设。

### 1.2 首席信息官制度

首席信息官(Chief Information Officer, CIO)制度诞生于美国,最早出现于美国的地方企业,后被政府机构引入。20 世纪 90 年代中期,为了加速军队信息化建设,美军参照地方模式率先在军队中实行 CIO 制度,并建立起了较为完善的 CIO 人才培养体系。

美国国会于 1995 年和 1996 年分别通过了《信息技术管理改革法》和《科林格—科恩法》,这成为美军设立首席信息官职位的推动力;美军又从自身信息化建设中吸取教训,急切拆除各军种“烟囱式”相互独立的信息系统、建立集成的军事信息系统,认识到战略规划、总体统筹对信息化建设的重



要性,这成为美军设立首席信息官职位的拉动力。通过一“推”一“拉”的内外刺激,美军先后在其三个军种部及其下属的一级司令部和五个战区司令部以及战略、军事运输、特种作战和联合部队四个专业司令部设立了首席信息官职位。

首席信息官队伍是美军建设全球信息栅格和综合军事信息系统的主要领导力量,目标一致但分工不同。国防部首席信息官主要负责顶层设计,制定全军统一标准、体制和政策;国防部各局首席信息官负责落实与执行;各军种部首席信息官负责本军种部分的设计与开发;各战区司令部首席信息官则负责反馈建设与使用信息,并提出作战理论指导建议。

## 2 我军信息管理组织体制存在的问题

当前,我军信息管理尚未形成规范化的管理制度,尤其在组织机构、领导体制建设上不够完善,相应的职能机构、组织结构以及人员配置不尽合理。信息管理组织的建设滞后,造成信息资源管理秩序比较混乱,领导关系不够明晰,运转不够顺畅;信息共享能力偏弱,信息“孤岛”现象严重,信息资源总体不足,还得不到有效利用;信息使用不规范,缺少统一的管理标准;信息基础设施建设重复投入,而整体效益不高的问题十分突出。主要体现在如下几个方面。

### 2.1 缺少总体规划,结构偏于简单

我军的信息管理主管部门主要是全军信息化建设领导小组、办公室和专家咨询委员会,各军区、各军兵种相应成立有信息化建设办公室,负责军队各级信息化建设。但是,各军种、军区负责各自信息业务的部门往往只在机关设置几个参谋、干事,负责整个部门的信息业务,下属各单位却很少设置专门负责信息业务的部门和人员。这种设置存在明显不足:头重脚轻,命令落实困难;层次模糊,职能不够明确;条块分割,存在管理盲区。

### 2.2 缺乏强制约束,发展过于随意

目前,我军信息管理组织机构仍然以“小组”、“办公室”命名居多,一方面,会给许多在军队成长多年的领导干部误解为是一种“非正式组织”,

另一方面,缺少正式的条文来规范组织行为。这就使得我军信息管理组织缺乏强制约束力,产生的现象就是各军种、军区各搞各的,你搞信息化,我也搞信息化,发展过于随意,造成各自为政,缺乏共同平台,指挥不顺畅的局面。各部门从自身角度出发考虑,倾向于自成体系,所建系统只求独立运转,不愿接受同级部门约束,这是造成“烟囱林立”的根源。同时,各单位总想保住本系统的“烟囱”,扩大业务管辖范围,争自己的发展权,也给管理、规范上带来麻烦。

### 2.3 缺少统筹兼顾,建设失于盲目

军队建设是一项系统工程,需要统筹兼顾,实现作战效益的最大化。当前我军在信息基础设施建设、组织建设上已经取得长足进步,但是仍然没有超出盲目建设的“怪圈”,重复建设、资源共享难和发展不平衡等诸多问题仍然严重存在。

### 2.4 缺乏建战一致,工作流于形式

当前,我军信息管理在组织机构和基础设施建设方面均比较薄弱,已有成果很难保证在实战中发挥实效,这也是各级主管部门特别是主要领导的“政绩意识”作祟的恶果。工作着眼点不高,只图眼前利益,喜欢表面文章等制约着我军从机械化向信息化转型的深化和发展。这需要各军兵种加强联系,建立兼容性好,保障到位的联络系统,牢固树立建为战的思想,坚持从实际、实战、实效出发,着眼提高信息化条件下的信息能力和工作效率,精心设计、精心组织、精心建设,做到以战促建、以用促建、建管并重,确保建一项、成一项、用一项,努力使各军种一体化联合作战成为可能。

## 3 我军构建信息官制度的必要性和意义

### 3.1 必要性:企业和政府先行,军队必须顺应潮流

美国自20世纪90年代开始在联邦政府和军队全面实施信息官制度,并取得了显著的效果。从发展的趋势上看,信息官制度首先是在企业产生的,用以管理信息化条件下企业的正常运作,即电子商

务时代；随后政府部门开始引进信息官制度，用以维持电子政务时代的政府日常管理运作；最后才是在军队实施信息官制度，这也是电子军务时代的产物。

国务院信息化办公室副主任杨学山在首届北大CIO班开学典礼上说：“无论是政府还是企业，信息化不成功的一个关键因素就是缺乏合格的CIO，这个缺乏不是一个小数目，而是一个很大的数目！”我国政府首席信息官职位和相关制度也已经在几个发达的城市和省份相继实施。1999年上海市启动首席信息官制度的试点；2001年江苏省政府启动首席信息官研修制度；2002年广东省政府明确提出建立信息主管制度；2003年北京市宣武区政府首次任命的43名处级政府首席信息官走马上任，等等。这些都充分表明我国政府主管部门和理论界正在不断地思考和探讨CIO设置的重要性，以及CIO在企业信息化进程中的作用等问题。

在我国企业和政府都逐步向信息官制度迈进时，军队应该紧跟步伐，融入到编制体制改革的浪潮中。20世纪90年代前期，美陆军改革着重在机械化重装师搞数字化建设，后来看出机动能力弱，不适应未来作战，便转过来搞“过渡旅”，由“过渡旅”进而转为“目标部队”，之后融入一体化联合作战部队。我军的信息化建设，应和结构改革相联系，先有结构合理化、再有信息化，起码二者要并行。否则，就可能落入“信息化陷阱”，出现“怪圈”现象。从长远看，不仅是人力物力的浪费，还将为未来的体制编制改革带来更大阻力。

### 3.2 意义：“师夷长技以制夷”

纵观世界各国电子政务的发展历程，建立首席信息官制度，由首席信息官及其相应的管理机构负责电子政务的总体规划、具体实施和全面管理，是比较通行和成熟的做法。《中国电子政务发展报告NO.3》指出：“目前，世界上已有一百多个国家和地区确立了CIO制度。各国正在积极推进的电子政务实际上是‘一把手’+CIO工程。”

信息化条件下的军队信息管理编制体制，肯定不同于机械化条件下的那套系统，甚至有可能否定一部分已经存在的内容，而伴随着电子军务产生的信息官制度无疑给解决这一难题打开了一扇窗户，这也是历史发展的必然趋势。同时，一直困扰我军

信息化建设的联合作战、未来平台建设等问题，都是因为缺乏一体化的领导组织体制来有效协调、统一规划，造成在互连、互通和互操作上的失衡，而信息官制度恰恰可以弥补这些不足。国外好的经验做法，我们应该认真地去琢磨，以彼之矛攻彼之盾无疑能在未来信息化战场的角逐中，有效捍卫国家和领土安全。

## 4 构建我军信息官制度的设想

所谓信息官制度，不同于以往我军在部队里设置的网管主任，通信站长之类职务，它是专职的、专业的、统领部队信息化建设的一个团队，拥有一定的行政权力，可以运用各种手段和工具来保证其管理、协调信息化过程中各项职能的实施。其中，主要负责人称为首席信息官，他是所在部队的决策者之一。

### 4.1 我军信息官体制

我军应在现有编制体制的框架内，按照“矩阵结构”模式，建立具有我军特色的首席信息官制度，完善各级信息管理组织部门，并使之与作战部门高度融合，为一体化联合作战构建作战平台提供组织保证。现阶段，在我军编制体制未有更大调整的背景下，我们认为军事信息管理组织结构也宜渐进式发展，结合现阶段我军建设的实际和今后几年的发展方向，我们认为在团以上单位和机关设立首席信息官，师以上单位和机关设置信息官办公室。全军信息化建设由军委统一部署，总参统一规划和管理，全军信息主管由总参谋长兼任，或设立一名专职副总参谋长，具体分管全军信息化建设事宜，通信部长在总CIO的授权下行使CIO职权。同时下设CIO专家咨询委员会和以CIO团队组成的信息官办公室，各军种、军区以及所属师以上单位分设信息官办公室。具体结构框图见图1。

其中，CIO主要负责所辖单位的信息化建设、制定战略远景和发展规划、协调各部信息化工作和组织具体实施。专家咨询委员会主要是为全军信息化建设的决策提供专家知识支持，从专业和技术角度客观无偏见地评判全军信息化建设规划、远景目标和具体的建设项目，并提出建设性意见和建议。各级信息官办公室由CIO和CIO团队组成，主要

协助本级主官实施信息化建设并提出咨询建议；研究制定相关指导性文件和法规；设计、运作信息资源管理的规程与方法；参与军事信息系统的采办管理和投资审查；制定信息管理人才培养计划并监督

其执行；提出信息技术装备开发项目的执行、修改或终止建议<sup>[6]</sup>。

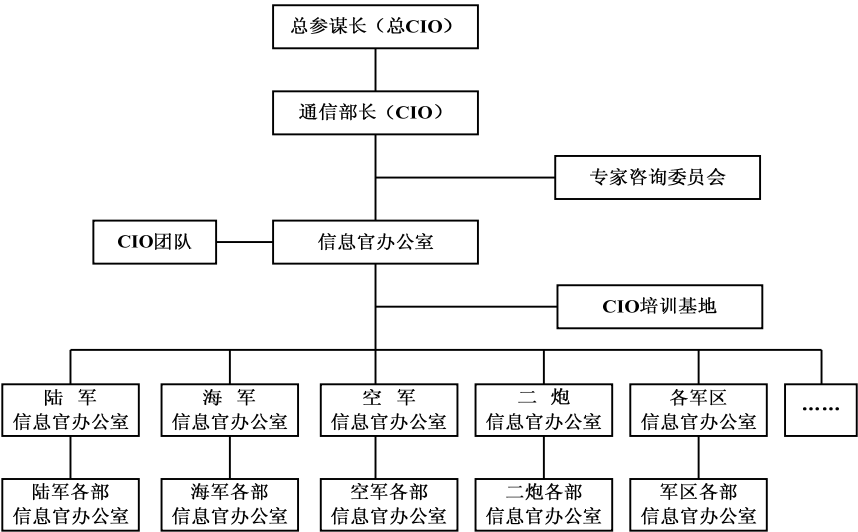


图 1 我军信息官体制结构图

4.2 我军信息官体制建设应该注意的几个问题

我军由于已经形成一套系统的编制体制，在实行信息官体制的过程中势必会产生一定的冲突和不适应的情况发生。因此，必须注意以下几个问题。

4.2.1 提高权限

CIO 必须具有权威性，参与部队战略规划制定和决策，一般是所在单位常委之一，从而有效克服“位低责高”的问题。目前信息官体制建设中遇到的困难，主要不是技术问题，而是实现预期目标所需的系统集成，资源管理如何协调的问题，这些问题如果解决不好，是无法实现既定目标的。

4.2.2 严格立法

信息官制度不是一个临时的机构，是需要长期

运行并需要正式法规规范的一项制度，在其开始发展的时刻，必须通过严格的立法实现其权限的最大实现和运行的畅通无阻。

4.2.3 成立团队

根据目前我国我军的形势看，现行教育体制还不能培养出全才以完全适应信息官职位的需要，所以必须有一个由不同知识结构的专家组成的团队来集体献策协助 CIO 的决策。

4.2.4 重视人才

信息官制度要求相应的人才培养机构的成立，即设置我军的 CIO 培训基地。这可以在国防大学设置 CIO 高级培训班，在通信院校或几所综合性大学成立 CIO 培训基地，为信息官制度输送专业人才。

参考文献（略）

作者联系方式

通信地址：陕西省西安市长安区王曲镇西安通信学院九队  
邮政编码：710068  
联系电话：15829765538

# 强化海军指挥信息系统组织运用 促进海军战斗力不断提升

魏荣亮 汪海波 李建伟

**摘 要：**海军指挥信息系统组织运用的实质，就是在一定的海军信息化组织运用管理机制下，对指挥信息系统各分系统综合运用的过程，是实现海军战斗力“聚合”与“倍增”的关键。因此，应以海军信息化指挥观念、指挥理论为指导，以实战需求为牵引，着眼发展，通过不断完善海军指挥信息系统组织运用机制、训练手段和系统保障能力，强化海军指挥信息系统的组织运用，促进海军战斗力的不断提升。

**关键词：**指挥信息系统；组织运用；战斗力

## 1 海军指挥信息系统组织运用原则

### 1.1 统一组织、整体协调

海军指挥信息系统分为岸基（固定式、机动式）指挥信息系统、舰载（编队、单舰）指控系统、潜载指控系统、机载指控系统等，设备类型多、种类杂，组织运用所涉及的范围广、协调难度大、协调关系复杂。因此，海军各级组织运用指挥信息系统，必须根据所担负的作战任务、首长的决心意图和指挥需要，统一组织、周密计划，合理确定系统的组成、配置和任务，统一协调系统各方面的力量，充分发挥各类设备、器材的作用，确保系统稳定、安全、高效地运行。

### 1.2 突出重点、把握关节

组织运用海军指挥信息系统，必须依托作战地域内三军既设通信网络平台，充分利用卫星、长波、短波、超短波、微波、散射、集群等多种通信手段，通过接入网关和交换设备多维接入，建立立体多路、纵横贯通的栅格状通信与指控网络，实现各级指挥所、作战部队、各作战单元之间的无缝链接，并集中主要力量，针对主要方向、重要时节和执行主要任务的部队，采取积极有效的措施，在人员、装备和组织上实施重点保障，对系统的主要网络、枢纽和关键节点等进行重点关照和把握，并根据需要调整技术保障力量，建立预备队，以应对意外情况的发生。

### 1.3 主动配合、密切协作

主动配合、密切协作，是保证各类系统保障力量协调一致行动，确保海军指挥信息系统有效运行的重要因素。针对不同的作战任务和战备活动组织，司令部、政治部、后勤部、装备部各相关业务部门必须积极协同，密切配合，做好系统的各项准备工作，组织系统运用时，各业务主管部门要树立整体观念，服从统一指挥，主动配合、密切协作，从全网全局出发，积极主动地解决遇到的各种问题。

### 1.4 体系灵活、流程快捷

组织运用海军指挥信息系统，必须从信息化条件下联合作战的实际需求出发，紧紧围绕海军作战指挥和遂行其他军事活动中复杂、多变的指挥关系及指挥方法的需要，按照海上作战扁平化指挥结构、网络化信息关系建立灵活的体系，实现信息流程的快捷，确保以岸基、舰（潜）载、机载等各类指控平台为中心，纵向贯通战略、战役、战术三个层次，横向上与其他军兵种指挥信息系统的互联互通，以实现兵力兵器高效灵活的指挥和控制。

### 1.5 严密防护、加强管理

构建一体化、实效的指挥信息系统，必须以确保指挥的稳定、顺畅为前提，采取一切有效的防护措施，搞好系统设施的工程防护、伪装和警戒防

卫, 增强“新三防”能力, 加强反侦察、反干扰以及防电磁脉冲、防计算机病毒和防反辐射武器摧毁等方面的措施, 形成全形态、全领域、全方位的信息防护体系, 确保系统人员、系统设施及信息的安全。同时要完善各种规章制度, 加强对系统值勤、电磁频谱、信道、安全防护、密码、装备与设施的管理, 以最少的资源代价使系统始终处于良好的运行状态, 确保系统效能的有效发挥。

## 1.6 平战结合、以战为主

随着信息化武器装备在战争中的大量使用, 作战节奏越来越快、持续时间大为缩短, 战机稍纵即逝, 对海军指挥信息系统运用的时效性提出了很高的要求。因此, 组织运用海军指挥信息系统, 要针对我军指挥信息系统既要满足作战需要, 又要服务于平时值班、训练、处置突发事件等活动的特点, 坚持“平战结合、以战为主”, 以能够同时满足战时、平时功能状态的需要, 突出战时运用, 加强对系统功能的熟练掌握, 加强对系统所需各种信息的获取、维护和管理, 加强系统各种保障的配套, 确保战时效能的发挥。

# 2 海军指挥信息系统组织运用中存在的主要问题

## 2.1 组织运用机制不合理

长期以来, 海军指挥信息系统的组织运用一直滞后于系统的建设和系统装备的发展步伐, 各级也尚未建立起完善的组织运用机制, 相关部门在组织运用和管理工作上的职责与分工也不明确。系统组织运用仍由各业务部门按照传统手段, 区分情报、侦察、通信、电子对抗、机要、航保等不同业务分块进行, “各业务部门纵向管理多, 跨部门横向协作组织少, 组织无序化; 各系统专项功能运用多, 通用功能运用少, 运用单一化; 系统终端单独运行多, 组网运行少, 运行单机化”, 增加了业务部门的负担; 同时, 也没能按照信息化条件下“感知、机动、打击、防护、保障”这五个作战行动要素进行系统的组织和运用, 有关数据采集、维护管

理、安全防护、抗毁重组、平战转换、应急运行、战训协作等一系列组织运用工作的机制还没有形成, 严重影响和制约了系统的使用及其效能的充分发挥。

## 2.2 训练水平不高

各级在针对指挥信息系统进行的组织运用和保障的训练上, 主动作为不够, 组训能力不强, 平时以武器系统或平台为主进行训练比较多, 以指挥信息系统为主开展的训练则很少, 大多数单位都不同程度地存在着等别的单位出经验、出成果, 等上级机关提供相应的训练指导材料, 然后借用现成的经验和指导来组织训练, 自己不主动去摸索和总结; 组织培训和学习, 主要以机关为主, 系统保障主要依靠厂家进行, 主动学习和研究不够, 对系统功能与能力掌握不全面, 组织和使用系统的能力得不到提高。对指挥信息系统缺乏信心, 习惯于使用传统的指挥手段, 驾轻就熟, 主动掌握和运用系统, 通过运用发现不足并改进系统的主动性不强, 严重背离了系统的建设初衷和效能的有效发挥。

## 2.3 系统保障不科学

指挥信息系统是建立在现代信息技术和信息资源利用的最新成果之上的, 涉及战场信息感知、通信与网络、信息对抗、计算机与软件等四大类 170 余种技术, 组织运用所涉及的技术保障工作十分复杂, 系统中各个分系统、信息网络和关键设备的任何一个环节出现问题或故障, 都可能影响到系统整体效能的发挥, 这对组织运用的保障提出了很高的要求。目前, 现行的保障体系和技术手段已不能适应海军指挥信息系统的建设实际和使用需求, 主要存在三个方面的问题: 一是与组织运行的机制一样, 区分不同的业务部门进行系统保障, 条块分割严重, 使得大量的公共信息在各分系统中重复地进行维护和更新, 增加了系统保障和维护的工作量, 迟滞了系统的快速建立、故障排除和恢复等, 严重影响了系统的有效运行和效能的充分发挥; 二是在系统保障上还以科研院所及技术厂家派员到现场提供技术和应用保障为主, 部队单独遂行保障的能力不足; 三是各单位现有技术保障人员大多是“半道

出家”，专业知识缺乏，并且，由于体制编制和用人机制等因素的不合理，造成了保障能力的不足。

### 3 主要对策

随着海军信息化建设的不断发展，海军指挥信息系统的组织运用、维护管理、技术保障等也面临着越来越严峻的挑战，成为制约系统作用和效益有效发挥的“瓶颈”，为解决好这个问题，抓好指挥信息系统的组织运用，为海军作战指挥提供更加有效、管用、实用的手段，推进海军军事斗争准备工作的落实，必须立足实际，做好以下几方面的工作。

#### 3.1 立足需求，完善组织运用机制

指挥信息系统效能的发挥，受到系统装备性能的左右，更依赖于系统的组织运用能力和保障水平。因此，必须以信息化条件下海军所面临的作战需求为牵引，更新观念，改变长期形成的以手工作业为主的传统指挥手段，强化指挥信息系统使用。需要强调的是，海军指挥手段建设和指挥信息系统的组织运用是一项有序的、动态的、可持续发展的系统工程，必须建立良好的运行机制，以促进建设和使用过程中各个环节的正规有序。所以，要把加强海军指挥手段建设和强化指挥信息系统的组织运用工作，列入到各级党委首长的重要议事日程，建立党委首长研究制度，定期听取有关工作汇报、分析研究本单位指挥手段建设情况和信息系统的组织运用情况，及时督促和协调各部门的工作，形成“首长——机关——部队”的组织体制，通过不断的建设和实际运用，逐步解决“不会用”、“不想用”、“不好用”以及使用效率“低”等问题，建立和完善的系统运用管理体制、制度、法规 and 规定等，把软件应用和数据使用突出出来，加速推进指挥信息系统各类软件的成熟及作战数据库的动态更新，并使其良性发展，形成规范，不断提高组织运用层次，提高各级组织运用指挥信息系统的能力。

#### 3.2 紧贴实战，扎实推进训练工作

海军指挥信息系统既用于平时，也用于战时，既要进入训练活动，也要进入管理活动，这既是

军指挥信息系统建设的初衷，也是不同于美军等西方国家军队 C<sup>4</sup>ISR 系统的特点所在。因此，海军指挥信息系统的组织运用，必须依据信息化条件下海军指挥体系，根据不同的作战任务和样式，按照作战指挥、情报、通信、军务、政工、后勤、装备等要素、设置和功能要求，安装相应软件，建立作战数据库，配置保密系统，围绕“侦、控、打、评”指控环路，从各类情报信息和指挥信息的获取、传递、分发、处理等关键环节入手，结合战备值班、处置突发事件，抓住训练演习和大型军事联合行动的时机，在实际兵力的配合下，组织和建立指挥信息系统，对系统开设的相关要素、组织运行方式、转进时机、相关保障等进行重点演练。从信息主导的角度出发，以加强信息系统操作运用训练为突破口，下大力组织联合攻关，强化实战背景下的训练，切实把应急作战联合指挥机构、指挥关系、信息流程搞清楚，提高指挥员和指挥机关对指挥信息系统的认识水平和运用能力，实现指挥与手段、技术与战术以及“人——机”系统的有机融合，提高指挥效益。

#### 3.3 着眼发展，强化系统保障能力

一是要加强管理，对各单位和部门的系统资源进行统一规划和调配，对现行各系统进行有效整合，形成统一的信息基础设施支撑平台，建立信息共享机制，盘活各类保障资源，从提高使用效益和保障效能的实际出发，立足科学发展，坚持作战需求牵引，采取整合提高的方式，确立先从业务系统内部整合，后对全系统保障资源进行综合集成的思路，实现各类系统保障资源使用效益的最大化；二是不断提高部队的系统保障能力，改变目前依托科研院所及技术厂家提供保障和支援为主的现状，形成“军民结合、部队为主”的综合保障体制，充分利用系统网络功能，综合采取网上保障、现地保障和后送保障等多种手段和途径；三是要实施人才战略工程，抓好人才队伍建设，建立人才培养、考核与激励机制，多方引进信息化人才，对于不能胜任信息化工作的人员要及时予以岗位调整，优化人才交流机制，对海军部队信息化人才统一调配，将优秀人才补充到重要岗位，为“人尽其才”打牢基础。为海军指挥信息系统的安全运行提供有效保障，

实现指挥信息获取的全面、准确、及时有效，确保 作战指挥顺畅。

#### 参考文献（略）

#### 作者联系方式

通信地址：广东省湛江市霞山区南海舰队司令部通信处

邮政编码：524001

联系电话：0759—2551110

# 对完善我军信息化组织领导体制机制的思考

孙海成 林华生 冯骞

**摘 要:** 本文围绕健全完善我军信息化组织领导体制机制问题,提出了建立垂直到底的信息化组织领导体系结构、健全我军信息化组织领导管理横向协调机制、加强和完善信息化建设技术领导等建议。

**关键词:** 军队信息化; 组织领导; 体制机制

推进军队信息化建设,关键在于有效的组织领导。目前,全军信息化组织领导管理体系已经初步建立,战略筹划取得重大进展,基本形成了信息化建设的统管局面,但规划计划执行难、重大决策落实难、跨领域和跨部门工作协调难等问题尚未得到根本解决。在这种情况下,抓紧健全和完善信息化领导体制和管理运行机制,有力发挥组织体系的保障功能,就成为推进我军信息化建设科学发展的关键。

## 1 建立垂直到底的信息化组织领导体系结构

自2003年全军体制编制调整以来,按照军委《关于成立全军信息化领导小组的通知》和《全军信息化专家咨询委员会组织方案》,先后成立了全军信息化领导小组,设立了全军信息化工作办公室,并组建了全军信息化专家咨询委员会。各大单位、海军、空军、二炮也先后建立了信息化领导机构和专家咨询委员会,以及军级部队信息化组织领导机构。这标志着我军信息化“三级”组织领导管理体系结构初步确立,适应我军信息化建设的新组织领导体制和管理运行机制正在不断健全完善之中。我军信息化“三级”组织领导管理体系结构,确立了在中央军委领导下,由全军信息化领导小组对全军信息化工作实施集中统一领导,四总部按照职责分工负责全军信息化有关工作;各军兵种、各军区按照本级职责,负责本级信息化工作;军一级单位按照本级职责,负责本级信息化工作的组织领导管理体制。各级要紧紧围绕我军信息化建设发展的战略目标,贯彻落实科学发展观和新时期军事战略方针,本着集中领导、统筹规划、综合集成、自

主创新、军民结合、确保安全的基本原则,进一步明确职能职责,统筹好当前与长远、全局与局部、纵向与横向、体系与要素等重大关系,努力推进我军信息化建设全面协调和可持续发展。但从目前我军信息化组织领导体制运行情况看,还有有待健全和完善之处。

### 1.1 建立师旅团级信息化组织领导机构

信息化建设是新军事变革的核心,是目前我军现代化建设的主旋律,是各级领导工作的中心。为保障这一中心工作的落实,各级都应建立强有力的组织领导机构。目前大部分师旅团级部队或单位还没有建立相应机构,致使信息化建设组织领导工作上下对口不畅,影响工作顺畅进行。因此,建议延伸信息化组织领导体系,建立师旅团级信息化工作领导小组,实现纵向领导体制的垂直到底。

### 1.2 普及首席信息官及首席信息官助理制度

首席信息官是美军实行的一种对信息化建设集中统管的领导制度。这一制度,对协调信息化建设各方面关系、统筹管理和高效推进信息化建设具有积极作用。借鉴美军经验,我军正在积极试行首席信息官制度。为使这一制度真正发挥效用,建议在普及首席信息官制度的同时,配套建立首席信息官助理制度。这是因为,为增强首席信息官的权威性,目前的首席信息官多为合成军首长兼任。但实践证明,由于合成军首长工作多和不太懂信息业务而影响了信息化工作的开展。因此,为趋利消弊,在首席信息官仍由合成军首长兼任的同时,建议为每位首席信息官配一名信息助理,该助理在首席信息官的直接领导下开展工作,代表首席信息官了



解、处理、协调相关问题，并为首席信息官提出各种咨询建议。

### 1.3 强化各级通信部门对信息化建设组织领导的支撑作用

目前，各级信息化工作办公室均编在通信部门，既体现了军委总部首长对通信部门的信任，又反应了通信工作对信息化建设的基础支撑作用。在这种体制下，如何处理好通信部门工作和信息化建设组织协调工作的关系，就成为能否互为推动、科学发展的关键。笔者认为，各级信息化工作办公室应在信息化领导小组的领导下，积极依托各通信业务部门开展工作；各级通信业务部门应坚决支持信息化工作办公室的工作，并在信息化工作办公室的总体协调下努力做好通信建设工作，以充分发挥通信对信息化的基础支撑作用，推进信息化建设的健康高效发展。

## 2 健全信息化组织领导管理横向协调机制

军队信息化建设的根本特征重在横向一体化，大量的组织协调工作是在跨领域、跨部门间进行的，传统单一的以职能部门为主体的纵向领导体制，已经难以适应和满足大量跨领域、跨部门的横向事务统管及协调处理。我军信息化“三级”领导管理体制的确立，为加强信息化跨领域、跨部门的横向事务统管及协调处理工作奠定了组织基础，但形成有效横向统管协调机制的问题尚未得到根本解决。深刻把握军队信息化建设本质特征，抓紧健全我军领导管理横向协调机制，尽快实现领导管理工作模式由重纵轻横向纵横一体工作模式转型，已成为完善信息化领导管理机制的关键。

### 2.1 成立综合系统建设横向协调机构

综合系统，是指根据信息化作战需求和信息化内在体系结构构成规定，由相关分系统组成的复杂巨系统。如指挥控制系统，就是根据信息化作战指挥需求和指挥控制系统内在构成规定，由指挥控制、情报探测、通信保障、测绘导航、水文气象等信息分系统组成的复杂巨系统。为适应综合系统建设需要，美军在国防部和各军兵种都成立了由主管

职能部门牵头，相关业务部门参加的横向协调机构，在国防部长或军种首长的统一领导下，牵头职能部门要围绕统一规划、组织实施、管理调控和进展评估等环节，形成统筹规划、各司其职、密切协同的运行机制。借鉴美军经验，根据各综合系统的组成结构和运作机理，建议以主管业务部门为主、四总部相关业务部门参加，成立各综合系统建设横向协调机构，采取平时分散办公、定期集中议事、建立联络员制度等方式，在军队信息化领导小组的领导和全军信息化工作办公室指导协调下，及时协调处理相关重大事宜，以完善信息化组织领导体制机制，适应信息化建设横向协调的突出特点。如成立由总参分工首长领导、总参信息网络主管部门牵头，四总部及海军、空军、二炮等信息部门参加的指挥信息系统建设横向协调机构；由总参分工首长领导、总参信息作战主管部门牵头，总参、总装及海军、空军、二炮等信息作战部门参加的信息作战系统建设横向协调机构。通过这些机构的横向协调活动，促进相互之间的信息交流，在统一的规划、标准和体制下，分工建设和同步发展综合系统，推动军队信息化建设的协调发展。

### 2.2 健全综合系统建设专家咨询机构

综合系统建设涉及各专业分系统，具有复杂巨系统特征。对综合系统建设的领导，主要是建设目标、建设思想、建设原则的和技术路线、技术体制、技术政策的确定。这些都需要先进的作战理论和信息技术做支撑。因此，为便于军委、总部首长的领导和决策，在充分发挥全军信息化专家咨询委员会作用的同时，应健全完善综合系统建设专家咨询机构及其职能，主要是针对某一方面（如指挥信息系统建设方面、信息作战系统建设方面、武器系统建设方面等）发挥专项咨询职能作用。新增的综合系统建设专家咨询机构成员，应以某一系统方面或系统建设领域里的一线专家为主，并适当吸收使命作战部队领导参加，形成总部领导、一线专家和部队指挥员相结合的具有研究论证咨询职能的机构。

### 2.3 加强横向联合总体性研究机构建设

一体化建设是信息化建设的本质特征，综合集成是信息化建设的基本方法。但综合集成不能仅仅理解为对已经形成的机械化“烟囱”系统的互联

和“作战平台”的互通，而是从研发源头就应贯彻综合集成思想，坚持信息化作战体系与体系对抗理念，着眼信息化战争“网络中心战”基本形态和一体化联合作战形式，聚合相关领域科研人员，集成各学科先进技术，进行联合开发研究。目前，我军信息化建设还没有完全从“门户式”利益观念、“烟囱式”科研体制、“封闭式”研发模式中摆脱出来，这与信息化建设的本质要求极不相融。因此，必须从科研体制和科研机制上进行根本性变革。建议在综合系统建设横向协调机构下面，对应成立若干由各相关分系统科研人员参加的总体研究机构。该机构应成为研究实体，而不是临时性或聚会式议论机构。在编制上应隶属于各综合系统建设牵头部门，业务上受各综合系统建设横向协调机构指导，以形成既有主管部门又能实现综合指导的科研机制。总体性研究机构主要负责综合系统作战需求的综合论证，重在综合系统的功能目标、总体结构和技术体制的总体设计，以及各分系统的功能目标、接口标准，并指导和检验各分系统的研发。各综合系统研究机构人员构成，应符合“三个综合”原则：一是应由该综合系统相关分系统的科研人员构成；二是应由作战部队、军队院校、科研院所专家构成；三是应由军事理论、作战指挥、科技研发、军事运筹、模拟仿真、军事经济等方面的专家构成。通过综合性的人员结构，集成各方面智慧，形成真正综合意义上的总体性研究结构。

### 3 加强和完善信息化建设的技术领导

技术领导是信息化建设的显著特征。信息技术及广泛应用是推进军队信息化建设的动力源泉。这一建设机理决定了必须加强技术领导。一体化建设、纵横集成、标准化接口等建设特点，决定了必须加强子系统的技术规范。战场的网络化结构、信息的网络化流动、力量的网络化融合等战场机制都受制于统一的控制系统，决定了必须强化对整个作战体系建设的技术监督。否则，军队信息化建设将未行自扰、不战自乱。技术领导不像行政领导那样依靠权威、靠令行禁止，而是要靠科学的总体设计、统一的标准规范、重大项目管理和严格的技术监督。

### 3.1 加强顶层设计，以科学的规划统领各分系统建设

信息化建设的顶层设计与机械化顶层设计有着本质的区别。虽然机械化建设也十分注重顶层设计，但其设计对象涵盖的仅仅是某一作战平台或某一独立系统的标准化。信息化建设的顶层设计注重的是体系标准化，其设计的对象涵盖各相关独立系统的复杂巨系统，要求顶层构想与实际需求相统一。加强信息化顶层设计，以科学的规划统领各分系统建设，是信息化建设规律的内在必然要求。顶层设计不但包括对综合系统总体目标、技术体制、标准规范和建设步骤，而且还应包括各分系统的功能目标、技术规范和完成时限等，以更科学的规划统领各分系统的建设，以严格的时间节点控制各分系统的进程，确保综合系统建设的健康发展。目前，随信息技术的应用日益广泛，我军信息化建设正由“技术驱动”为主向“需求牵引”为主转变，应用主导明显增强，但需求论证尚缺乏科学规范，特别是对主战武器和信息系统建设的总体需求论证严重不足，致使一些系统建设效益低和难以取得突破性进展。缺乏科学顶层设计是其主要原因之一。如何深化需求研究、完善顶层设计，已成为当前必须认真研究的重大课题。我们认为顶层设计应由横向联合的总体性研究机构承担，由综合系统建设横向协调机构审议，由总部职能部门报军委研究决策。一是要抓紧论证我军信息化建设总体需求体系。按照当前需求与长远规划有机结合的要求，力求作战需求目标化、建设需求任务化和实施行动方案化。二是尽快完善可以量化、具有操作性的信息化建设目标体系。当前，要抓紧2010年、2020年前第一、二阶段目标的研究论证，以明确具体的目标牵引我军信息化建设发展。三是抓好《军队信息化建设规划纲要》等相关文件的贯彻落实。适时检查指导各项重点工作和建设项目进展情况，及时发现问题、纠正问题、反馈情况，确保各项建设保质保量按期完成。四是抓紧制定与国家信息化相协调发展的策略。把军队信息化建设发展战略尽快纳入国家信息化战略体系，实现与国家信息化的互补性发展，促进军队依托国家信息化的跨越式发展。

### 3.2 加强标准建设，以统一的规范指导各分系统建设

标准是信息化建设的生命。没有统一的标准，网络无法互联、系统无法互通、信息无法共享。标准制订必须超前，否则将影响系统建设。标准必须科学、精确和统一，否则将造成系统混乱。业内流行的“三流企业卖产品、二流企业卖技术、一流企业卖标准”，已足以说明标准在信息化建设中的地位。这就要求各级信息化建设管理部门和综合系统建设职能部门，高度重视标准建设和管理工作。当前，应尽快建立起一套科学、先进、合理、准确、实用和可操作性强的技术体制和标准，这是我军信息化建设的一项十分紧迫任务。全军及各大单位信息化工作办公室应把各项标准规范的制订、颁发、检查、测评等工作作为重要职能，通过“标准”这个法宝，统一规范各分系统建设，指导和管控全军信息化建设工作；各总体研究机构要把标准制订作为顶层设计的重要内容，通过标准规范各分系统建设；各综合系统横向协调机构，应把标准审定作为重要内容，通过标准协调解决各分系统之间的有关建设问题。要统一全军信息编码工作，制定全军信息编码体系，建立编码统一的全军各类信息数据库，提高信息共享能力。

### 3.3 加强立项审查，以严格的程序保证决策科学水平

与外军相比，目前我军信息化的科学决策辅助手段差距还很大，致使许多重大问题决策缺乏科学的定量分析和战略评估，由此决定了我们在一些重大问题、重大项目的决策问题上，更要注重科学性、可行性和统一性，提高规划计划和重大决策的科学化水平。特别是对战略性、基础性、周期性的重大问题和重大建设项目，必须建立决策审查和滚动修正机制，以前置的审查关口确保重大问题和重

大建设项目的决策质量效益。比如，发展目标和任务安排是否符合我军信息化建设规划纲要的规定要求；技术体制是否符合军队信息化一体化技术体系结构的规定；重大项目设置和调整计划安排是否与相关项目、计划协调配套，避免了重复建设；重大项目的可行性论证和风险评估是否充分，配套措施是否完善等问题，都需要由全军信息化专家咨询委员会组织专家进行审查，形成审查意见后，才能提交全军信息化领导小组审定或呈报中央军委审批。各总部、各大单位呈报中央军委审批的规划计划类文件中的信息化内容和信息化新建、调整、综合集成建设项目（包括工程建设项目、装备建设项目、专项工程项目）的立项，应当经由全军信息化领导小组审议审定。立项审查工作，应由全军信息化工作办公室按照《军队信息化建设规划计划和重大项目立项审查实施办法》规定的程序承办和处理。

### 3.4 加强技术监督，以全方位的监测约束各分系统建设

技术体制和标准，是武器装备建设的法规。为避免目前装备发展存在的同型号装备却电路图纸不同、同一电路图纸装备却面板配置和内部结构不同、同一连接关系却接口标准不同等现象发生，必须全方位加强综合系统建设的技术监测，确保综合系统及其分系统建设在严格的监控约束之下，切实防止执行技术体制和标准不一、质量标准参差不齐等问题的发生。各综合系统建设均应成立技术监督小组，设在总体性研究机构内，上对综合系统建设职能主管部门负责、下对各分系统建设实行技术监督。技术监控应全程实施，特别是在各分系统预研、立项、成果审定、样机生产等阶段，更应全面检查验收。技术监控必须以系统的总体设计和标准法规为依据，在总体规划统领和标准法规规范下，制定若干检测验收、测评标准，确保监控工作的精确实施。

参考文献（略）

作者联系方式

通信地址：通信指挥学院发展战略研究所

邮政编码：430010

联系电话：13329733115

# 军事电子信息系统建设的需求问题浅析

彭慧军 蔡力强 赖旻

**摘 要:** 本文从军事需求的概念入手, 结合我军电子信息系统建设的实践, 针对一体化联合作战对军事电子信息系统的客观要求, 侧重于作战需求总体层面, 指出了军事电子信息系统建设中作战需求方面存在的问题和差距, 力争从深层次、次深层次分析问题产生的原因, 探索、总结系统建设和研究中的需求规律, 进而提出解决问题的对策与方法。

**关键词:** 军事电子信息系统; 需求; 对策

## 1 引言

军事电子信息系统是在信息时代的军事环境下, 为形成武装力量体系对抗优势, 利用综合集成途径研制的复杂巨系统, 具有高动态性和难以控制的整体性、对抗性和多样性的特点。已经从传统意义上的保障和配套装备发展成为支持多军兵种联合作战的核心装备。

军事电子信息系统建设从明确需求开始, 到实现需求终结, 需求工作贯穿于系统建设始终, 是系统建设的前提和基础, 对系统的开发、研制起着导向、牵引、检验和增益的作用。直接关系到系统建设的成败。

军事需求的概念是“对确定研制的新型武器的作战使用和技术性能所提出的要求。包括承担的作战任务、战术性能、使用价值等, 是新型装备研究设计、试验和定型的基本依据”。美军认为, 需求是“提出采用什么手段或获取何种武器来完成特定领域的作战任务”。可以说, 作战需求是指作战对军事电子信息系统提出的一系列有关系统功能、性能和操作环境等方面的要求, 从结构上可分为三个层次。军事需求, 即作战对信息系统的需求。主要是从军事使用部门的现实作战需要出发, 确定信息系统建设的目标、作战背景、作战任务、指挥特点、指挥方式、指挥体制、指挥程序对系统的特殊要求等; 系统需求, 即分析后的需求, 是将军事需求进行功能分解而形成的系统各种功能、结构需求的概括, 包括功能划分、物理组成、接口关系及信息流程等方面的需求; 技术需求, 即系统需要遵循的技术条件, 是在理解应用的功能、结构需求的基础上确定的技术要求。

军事电子信息系统的需求随着电子信息技术的迅速发展, 联合作战的要求不断提高, 呈现出主体不明、边界不清、建设过程渐近的诸多特征, 具有不确定性、长期性和时变性。传统的“系统工程”方法似乎很难适应军事电子系统的开发。因此必须运用工程化的方法, 科学合理的实施需求定义、论证、分解、推演、改进及管理等一系列群体参与的过程, 全面认识联合作战对各种综合电子信息系统的客观需求, 切实发挥对装备研制和系统应用的指导促进作用。

## 2 问题

目前, 我军信息化建设正处在一个转型的快速发展时期, 已建和在研的各级各类军事电子信息系统对军事转型和我军作战能力的提高无疑具有重大的促进作用。但是, 由于缺乏大型信息系统建设的经验, 对需求牵引在系统建设中的作用意义认识不足, 亦没有被摆在正确的位置, 致使需求问题成为系统建设的又一瓶颈。概括起来, 主要有如下方面。

### 2.1 需求主体

军事电子信息系统的建设, 必须要有清晰的指导思想 and 建设目标, 而明确的需求主体是系统建设的重要基础。目前军事电子信息系统建设的一个突出问题是需求主管部门不明, 职责权限不明。需求主体是科研管理部门、建设单位、还是使用单位? 或者为三者之结合? 这些在以往的建设中没有明确和界定, 加之缺乏法规、条例和相关标准, 致使需

求工作无章可循、无据可依、无前可鉴，在一定程度上影响和制约了军事电子信息系统建设。

## 2.2 需求过程

完整的需求过程应包括：需求培训、需求获取、需求分析、需求规格说明、需求验证和需求管理等。是依托管理和技术支撑，经历分析——设计——验证的螺旋式上升过程。从以往的情况看，这个基本的需求过程并没有被多数开发单位采纳。需求获取手段和方法单一；需求过程随意，只重视结果，忽视过程；没有进行过需求培训；不能提供科学有效的需求测试和需求管理。过程的缺乏导致作战需求滞后于科研开发，致使需求在科学性、完整性、可操作性等方面均距可牵引系统工程建设的标准相差甚远。许多大型系统都是边提需求，边开发，时常出现科研开发等需求、改需求的状况。

## 2.3 需求交互

军事电子信息系统建设的一个现象是：建系统的人不用系统，用系统的人很少参与系统的建设。在设计开发阶段，直接用户，如作战、通信、情报、兵种等指挥参谋人员因其繁忙的战备训练工作，不能全过程地参与系统建设，需求人员不能相对固定，且变动频繁。由于不能及时、实时地进行交互，或交互的站立点不一致，研发人员只能按照自己的理解完成设计和开发。致使问题堆积，在开发前期即可能产生了方向性需求偏差，而这种偏差又会持续整个研发过程。修复这些偏差不仅耗时耗力、成本巨大，而且使系统的实用性受到很大影响，系统的效益不能有效发挥。

## 2.4 需求描述

需求描述是对获取的军事需求进行精确化格式化描述。作为用户和开发者之间的一致协议，其描述应该简明、易懂、无二义性。由于大多采用自然语言而不是形式化语言进行需求描述，其多义、模糊和二义性使不同的读者难以达成相同的理解。军事电子信息系统用户假定读者具有相关特定军事知识，所以需求文档和规格说明没有包括必要的解释信息。描述不清晰，需求文档定性的内容多，定量的内容少，提供给开发人员可供编程的内容和可操作性欠缺。所有这些致使建成后的系统与作战需求

描述的要求差距较大。

## 2.5 需求管理

主要表现在不能对需求工作进行科学有效的管理。需求开发中，需求收集和系统分析时间比例关系被颠倒。很多军事电子信息系统仅完成少量的需求获取和收集工作后，就把大量的工作都放在了系统分析上。正确的方法是最初只完成少量的系统分析工作，大量的工作放在分析和验证需求上。随着系统开发过程的推进，需求收集与系统分析的重叠会发生变化。但由于前期需求收集花费的时间较少，使得系统分析所要求的需求指标达不到开发要求，不得不把工作重心又重新转到需求收集上，浪费大量时间和经费，如图 1 所示。其次，对需求缺乏全过程管理和用户对需求的随意性变更也反映了在需求管理方面存在缺陷。

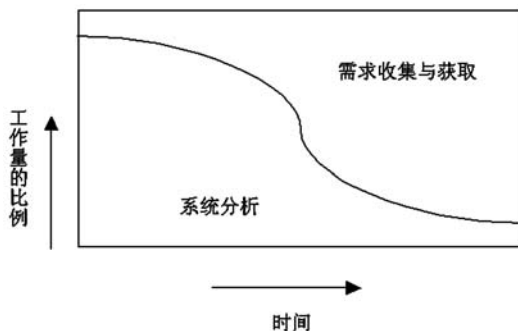


图 1 需求收集与获取和系统分析的比例不当

## 2.6 需求验证

需求验证是指利用需求描述验证工具和需求验证方法对军事需求进行描述符合度和需求信息完整性两个方面的验证。从目前看，多数需求由于受时间、职责、任务等多种因素的制约，没有进行较为系统、正规的需求评审和验证，或者需求评审验证流于形式。测试流程与作战流程吻合程度不高，测试过程注重单项功能的测试，忽视了一体化、综合性、多军种的综合测试，测试用例欠缺战术背景等。

## 3 分析

上面列举了目前军事电子系统需求工作的主要问题，产生这些问题的原因是多方面的，综合起来

主要有:

1) 没有权威的作战需求组织管理协调机构。需求研究的规模小且是局部、分散的,需求研究既缺乏统一整体的规划和指导协调,又无法服务于科研,没有实现需求资源共享;既缺乏需求研究的针对性、权威性,更难指导科研工作地开展。

2) 缺乏统一的作战需求研究规范、工具、标准和有关规定。由于我军正值机械化向信息化转型期间,缺乏规范化、形式化的军队信息化建设需求描述工具;缺乏有效工具对需求的一致性、正确性、完整性等进行分析和验证,致使需求的可信性和可用性得不到保证;需求管理方面也多采用商用需求管理工具软件,缺乏适合军队信息化建设的需求管理工具,需求研究和分析的方法滞后于科研开发。

3) 缺少专业的军事需求分析人员。由于缺乏需求管理机构和配套的管理机制,需求分析队伍的

建设与管理处在无序状态。多数需求分析人员不是专职,对未来的联合作战、军兵种间的协同作战需求的了解缺乏深度,指挥员、技术人员结合不紧密,难以对科研工作形成有力的指导。

4) 作战需求研究论证的投入力度不够。由于对军事需求研究的重视程度不够,军事需求研究在型号研究工作中没有专题的研究要求和专项经费,缺乏统一的组织协调,不注重军事需求工程化的建设投入,需求工作经费在系统研发中所占比例偏低,难以支撑工作的正常展开和顺利进行。

图2是采用系统工程之因果分析法对军事电子信息系统的需求问题进行的系统诊断。根据军事电子信息系统建设的客观情况,在对已获得数据进行补充的基础上,对需求问题进行了归纳,从以下6个方面分析找出问题的原因,旨在为提出解决和改进的方法提供有价值的依据。

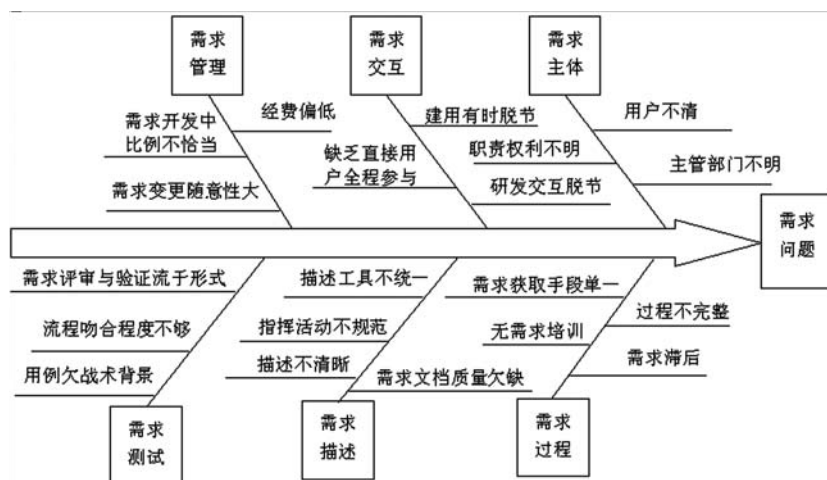


图2 军事电子信息系统需求问题因果分析

## 4 对策

### 4.1 成立需求研究管理认证机构

需求工作,是一项复杂的系统工程,有一个渐进滚动发展、系统研究和不断积累的过程,需要在统一规划下有序地管理和组织协调。目前我军尚没有权威的军事需求研究管理和认证机构,亟需从组织上对作战需求建设给予保证。其意义在于:

1) 信息化军队转型建设的迫切需要。我军当前正在从合同作战走向联合作战,由机械化向信息化转变。这就要求把各军种相互封闭的、纵向直统的作战体系转变为开放的、横向互动的作战体系。

因此,建立作战需求研究论证机构,统一一体化的应用视图,提供兼容性、连通性、共享性和互操作的基础结构,其意义在于理清信息化、一体化建设的最大共享范围和互操作性,以及对未来可持续应用与发展的适应性。

2) 保障我军遂行联合作战任务的客观要求。一体化联合作战将是我军未来作战的主要作战形式,这就对信息系统互连互通和体系结构的设计提出了更高的要求。一体化联合作战,作战体系根据任务需要,对各军兵种军事电子信息系统进行模块重组,指挥自动化作战体系结构是基于基本作战结构的拼装来“搭积木”,从而要求作战体系结构灵活变化,而且具有与不可预知的信息系统组合使用

的通用性和互操作能力。因此,在联合作战时代,必须要有一个作战需求研究论证机构和管理体制,统一提出和管理多军兵种联合作战的信息系统作战需求,以适应三军最大共性基础和无缝互操作,符合联合作战对系统的兼容性、扩展性和其他要求。

3) 大型信息系统项目实施的关键环节。从我军多个大型信息系统存在的问题分析,对作战需求的研究论证不透彻,作战需求不清晰,牵引力度不够等需求问题,已成为制约我军信息化建设的瓶颈问题之一。建立作战需求研究论证机构,提出、研究、分析作战需求,协调指导系统工程建设,是确保信息系统实用性的重要保障。总之,建立需求研究论证机构有利于对信息系统建设实施有效的宏观调控,有利于使信息系统建设适应联合作战的客观需要,有利于促进信息系统建设顺利发展。

需求论证研究机构的工作职责:组织对军事电子信息系统的作战需求进行论证、认证,提供先进的需求获取手段,支持需求论证分析人员利用工具调查、咨询、座谈、用例和场景等方式获取需求;提供规范化、形式化的军事电子信息系统需求描述工具,解决目前基本采用自然语言或商用需求工具软件描述系统需求的问题,能够全面、准确、规范地描述军事需求,生成需求规格说明;依据需求分析评估标准和评估模型,实现对各种需求的一致性、正确性、完整性进行分析、评估与验证,确保需求的可信性和可用性;提供可捕获、跟踪与管理需求工程过程中的各种需求及需求演化进程的工具集,支持需求变更影响分析和需求版本控制。

## 4.2 规范需求工作

需求牵引,说到底还是作战任务牵引。只有对未来作战做出贴近自己实际的描绘,才能提出准确、科学、全面、清晰的需求。本文所指的规范需求工作包括三个方面,即规范指挥流程,规范需求内容,规范需求描述方法。

### 4.2.1 规范指挥流程

完整规范的指挥流程是军事电子信息系统设计研究的依据。一方面,规范的指挥流程可以便于技术人员理解基本作战行动,建立一套全军共享的、无歧义的联合作战行动视图,从而在军事人员、技术人员之间建立无缝的交流界面。另一方面,军事电子信息系统要支持指挥人员完成信息化条件下作

战指挥活动,反过来必然对作战指挥流程提出新的、更高的要求。未来信息化作战将由按时间表进行的被组织协同,变为依信息流进行的自组织协同;由程序化、程式化的线式作战,变为非程序、非程式的非线式作战。军事电子信息系统要求作战指挥流程相对规范。同时,还要求在指挥活动中除了基于作战指挥一般程序中包括的了解任务、搜集情报、判断情况、定下决心、制定计划、下达作战命令、协调控制部队行动、战场情况反馈外,还要总结提出基于一般程序、适应作战指挥需要的规范流程。美军由顺序作战发展到并行作战,正是因为有规范的指挥流程做基础,使其信息系统的研制少走了很多弯路,在近几场战争中得到验证。从我军历史看,尚无大规模联合作战的经验,信息化条件下联合作战的指挥流程必然成为需求研究的关键。因此,我们要以《联合战役纲要》、《司令部条例》等条令为基本依据,参照我军演习训练等实践活动,分析传统的指挥流程距高技术条件下作战要求之差距,按照军事电子信息系统对指挥活动的要求,规范指挥活动和指挥流程。

### 4.2.2 规范需求内容

军事需求是从军事使用部门的现实作战需要出发,确定系统建设的目标,研究系统所处的作战背景,包括作战环境、作战编成、作战样式、作战特点及对系统的影响,以及指挥活动、指挥特点、指挥方式及对系统的特殊要求,是系统的顶层需求。它反映了作战对军事电子信息系统的客观要求,是系统功能、结构和技术要求的基础,是分析论证系统总体需求必须要解决的问题。军事需求的内容很多,但重点是关键需求。关键需求是系统需求中抽取的反应系统本质的一个子集,即绝对必要的需求。军事电子信息系统的关键需求包括基础性需求、指挥性需求和掌控性需求。基础性需求是军事电子信息系统必备的基本条件,指挥性需求是指能为实施统一有效的组织指挥提供必要手段,掌控性需求是指系统能为准确、实时的掌握敌情、我情、战场情况提供必要的技术支持。具体包括使命任务、作战样式、作战编成、作战指挥流程、作战指挥关系、系统功能要求、系统性能要求、约束条件、非性能需求和综合保障要求等。

### 4.2.3 规范需求描述方法

规范的需求规格说明应该具有以下的特点:



① 完整性。不能遗漏任何必要的需求信息,遗漏需求将很难查出。注重用户的任务而不是系统的功能将有助于避免不完整性。② 一致性。一致性是指与其他软件需求或高层需求不相矛盾。在开发前必须解决所有需求间的不一致部分。③ 可修改性。在必要时,或为维护每一需求变更历史记录时,应该修改规格修订说明。这就要求每项需求要独立标出,并与别的需求区别开来。④ 可跟踪性。能够及时准确地跟踪每一项需求的源头。

需求的规范化描述需要相应需求描述工具集的支持。需求描述工具集对得到的初始需求进行严格的形式化或规范化描述,辅助需求论证人员分析初始需求提出的各种问题,提出解决方案,并从多个视角进行描述。需求描述工具集包括业务需求描述工具子集、组织需求描述工具子集、信息需求描述工具子集、系统需求描述工具子集、技术需求描述工具子集和非功能性需求描述工具子集等。

### 4.3 构建军事电子信息系统需求分析与评估环境

建设统一的军事需求分析与评估环境用于对军事电子信息系统的作战需求进行获取、分析及验证,这是需求工程的重要环节和必备条件,有助于强化顶层设计和需求牵引,提高系统的实用性,对加速我军军事电子信息系统建设具有十分重要的意义。军事需求分析与评估环境的作用为完成需求获取、分析、评估、管理和系统建模、能力描述、编配应用研究制定、需求知识库建立与管理,为军事电子信息系统需求分析提供规范的、有效的分析和验证评估手段与环境;同时,用于支持在体系对抗背景下军事电子信息系统建模时的需求分析,支持需求分析后的迭代验证评估,支持进一步的电子信息系统设计,降低在系统开发时所面临的风险,也利于信息化作战概念、理论的创新、发现和设计。其具体用途为:提供先进的需求获取手段,解决目前基本采用自然语言或商用需求工具软件描述系统需求的问题,提供规范化、形式化的军事电子信息系统建设需求描述工具;提供有效工具对需求的一致性、正确性、完整性等进行分析和验证,保证需求的可信性和可用性;为军事电子信息系统建设项目需求论证与评估提供环境支持和方法保证。具有需求获取、需求分析与评估和需求管理功能,由需求获取、需求分析与评估、需求管理等工具软件和

需求知识库构成。需求获取支持需求论证分析人员利用工具调查、咨询、座谈、用例和场景等方式获取军队信息化建设需求;提供规范化地描述需求的工具集;需求分析与评估制定需求分析评估标准,建立评估模型,支持对各种需求的一致性、正确性、完整性进行分析、评估与验证;需求管理提供可捕获、跟踪与管理需求工程过程中的各种需求及需求的演化进程的工具集,支持需求变更影响分析和需求版本控制。

### 4.4 强化需求验证与评估

需求验证与评估是需求工作的重要过程,用于检验需求的科学性、正确性和合理性,判断需求是否符合我军实际和能否达到研制目标。针对目前存在的需求验证与评估流于形式及与作战吻合度不高的问题,我们必须大力强化需求验证与评估工作,应着重把握以下三点。

1) 要提高需求验证与评估的重视程度。首先明确需求是必须测试也是可以测试的,如果发现系统某一个需求是不可测试的,那么它能否被正确地实现将是一个问题。严格正规的需求验证与评估能够牵引系统建设,并能够在早期及时发现系统中存在的问题,避免因需求偏差产生的巨大损失。我军和外军的成功经验和失败教训都清楚表明了需求验证评估对于系统建设的重要作用。

2) 要采用科学的验证评估方法。可采用正向需求跟踪和逆向需求跟踪两种方式,正向需求跟踪是指由需求描述出发,得出系统对于该项需求的实现与维护;逆向需求跟踪是指由系统功能可以追溯到该项需求的原始出处。不论是正向需求跟踪还是逆向需求,应能在每项需求与它的根源和设计元素、实现、测试用例之间建立起链接。

3) 确保需求验证评估的质量。在我军没有实战环境检验的情况下,构建带有战术背景的近似实战的作战想定、战斗方案模型、测试用例是实现测试目标的重要途径。通过有作战主体用户参加的,基于完整作战指挥流程、具有战术背景的测试来确认系统的需求。

4) 确保需求验证评估贯穿于研制全过程。军事电子信息系统是一种集软硬件为一体的、复杂的人机交互式系统,不仅需要相关的技术领域和业务领域知识,还涉及语义学、认知科学、行为科学等交叉学科知识。军事电子信息系统的需求测试不仅



存在于方案设计阶段，也存在于系统设计、系统验收阶段，要进行需求验证评估、系统集成测试、系统综合测试和模拟演示、实兵演习检验，是一个不断迭代、反复进行的过程。

## 5 结语

军事电子信息系统需求工作，必须有科学的需求开发方法，统一的规范标准，有效的开发和管理工具，基本的环境和验证手段做支撑。应该欣喜的

看到，本文所总结的需求问题已经逐步引起人们的重视，需求工程对于军事电子信息系统建设的意义，需求管理认证机构，军事需求分析与评估环境等方面也已受到广泛关注。需求问题必将会随着我军信息化建设的深入发展而得到解决。我们需要认真分析、总结我军电子信息系统需求工作现状，找准薄弱环节，提出解决对策，搞好顶层设计，建设符合联合作战需要的军事电子信息系统，为推动我军信息化建设又好又快的发展提供支持。

## 参考文献

- [1] 李德毅著，发展中的指挥自动化，北京：解放军出版社，2004.10
- [2] 戴浩编著，军队指挥自动化建设研究，北京：国防大学出版社，2005.4
- [3] 戴锋编著，现代系统工程，郑州：河南人民出版社，2001.10
- [4] 军事科学院，美军联合作战新构想，北京：军事科学出版社，2005.7
- [5] 王积鹏，“从体系工程”方法入手，探索综合电子信息系统的发展规律，国防信息化，2006.4
- [6] 刘俊先，姜志平等，指挥信息系统需求描述框架研究，军事运筹与系统工程，2006.12
- [7] [英]罗伯逊著，王海鹏译，掌握需求过程，北京：人民邮电出版社，2003.2

## 作者联系方式

通信地址：北京市丰台区大成路 13 号院 Z01

邮政编码：100039

联系电话：010-66820126

# 欧洲军队信息化建设现状与启示

卜格鸿 赵洪利 王英华

**摘 要:** 欧洲强国新军事实力强大, 信息化建设有一定的经验。从经济基础、工业基础、军工体系、信息产业等方面分析欧洲强国军事优势, 研究法国、俄罗斯、英国、德国和瑞典等国的军事信息化现状, 提出加速升级现有武器装备及平台、运用尖端信息技术综合集成武器系统和发展我军的信息网格等思路。

**关键词:** 欧洲; 装备信息化; 现状; 启示

欧洲在 2005 年和 2006 年世界新军事实力前五名荣占三个席位, 分别为法国(居美国之后)、俄罗斯(第三名)和英国(第五名)。以法国、俄罗斯、英国、德国和瑞典等为首的欧洲国家目前陆、海、空单件武器装备基本实现了信息化, 信息化武器装备占装备总量的二分之一以上, 与美军不相上下。目前西方强国大多数武器装备的电子信息技术成本比例已超过 50%。资料表明, 欧洲强国正在加速武器装备信息化建设, 即利用信息技术和计算机技术, 使预警探测、情报侦察、精确制导、火力打击、指挥控制、通信联络、战场管理等领域的信息采集、融合、处理、传输和显示联网, 实现自动化和实时化; 正在加快装备各级军事信息系统, 即列装信息技术含量高、信息起主导作用的作战武器和保障装备, 主要包括军队的 C4ISR 系统、信息化作战平台、智能化弹药、智能机器人、数字化单兵系统等; 正在加强各军兵种武器装备一体化程度和互联互通能力; 正在加紧建设战略级侦察预警系统, 因此作战能力日趋提高。

## 1 欧洲强国军事优势分析

欧洲强国军事优势的原因有很多, 主要原因有五方面。① 强大的经济基础足以维持其装备精良的高技术军队。近几年来瑞士、荷兰、瑞典等欧洲国家全球竞争力排名一直高居榜首。世界经济论坛公布的《2005—2006 年全球竞争力报告》和《2006—2007 年全球竞争力报告》显示, 欧洲国家在前十名中占有大多席地位。这些欧洲国家在宏观经济管理方面表现出色, 政府对维持良好的公共财政有很强的责任感, 实现预算盈余, 对军队的信

息化建设投入巨大。② 雄厚的工业基础支撑军事科技的发展。法国、英国、德国等欧洲国家具有雄厚的工业基础, 民技军用渠道通畅, 材料供应和工艺精湛有良好的保障。俄罗斯重工业基础雄厚, 军事科技发达, 拥有很强的武器自主开发能力, 其自行研制的 SS-27 “白杨”核洲际导弹的弹头再入大气层时, 能作 S 型机动, 令美国 NMD 拦截系统束手无策。③ 完善的军事工业体系保障武器装备建设。经过第二次世界大战的洗礼, 欧洲强国都具有完备的军事工业体系。武器自主开发和生产能力强。如法国军事装备几乎不依赖别国, 能够开发出很多和美国分礼抗庭的高技术武器, 其自主开发的先进战略核潜艇、中程核弹道导弹和美国相比, 差距不大。德国军事工业的研究和发展重点已放在了系统技术和尖端技术上, 特别是在指挥系统和武器使用系统方面强调应用传感技术和电子技术。④ 发达的信息产业促进武器装备信息化建设。欧洲强国社会信息化程度高, 国民信息素养好, 国家信息基础设施完善, 掌握核心信息技术。拥有发达的民用高科技的同时, 尖端军事技术日新月异。⑤ 追随美国军事提升军事实力。除俄罗斯以外, 欧洲强国大多是美国的同盟国, 他们追随美国及时启动了 C4ISR 系统, 在军事信息化建设和军事行动上多有横向联合与互助, 这也是欧洲强国保持军事优势的一个原因。

## 2 欧洲强国军队信息化现状

### 2.1 横向技术一体化的大思路

欧洲强国军队目前为发展信息化装备确定的大

思路主要是“横向技术一体化”。以前,各国装备建设的基本模式是:利用最新、最先进的科学技术,从纵向上研制一代比一代射程更远、精度更高、毁伤力更强的武器系统。采用这种传统的、“烟囱”式的武器发展方式,时至今日,已使许多武器装备的射程、速度、杀伤力、精度等性能指标达到或接近达到物理极限。“横向技术一体化”则要求利用现有的民用和军用技术,用共同的软件、标准和规程,从横向上对现有武器系统进行现代化改造或改进,使其具备通用性、联动性,从而更便于从传感器到射手之间、各武器系统之间、各作战部队之间的信息流动,大幅度地提高所有武器装备和作战系统的整体效能。

依照“横向技术一体化”大思路,欧洲强国在加速装备信息化进程中应用“贴花”的方式,给原有的坦克、装甲战斗车、大口径火炮、武装直升机、作战飞机和舰艇等主战装备,加装数字化通信设备、先进雷达、敌我识别装备和全球定位系统接收器。俄罗斯军队的大多数武器装备都达到了机械化发展的极限,所以其武器装备信息化建设的起点很高。俄军和法国已把加强武器的通用化、标准化、规格化,减少武器的种类,作为装备建设的一项重要方针。俄军有针对性地提出了发展陆军侦察一打击一体化武器系统计划。该计划主要针对炮兵装备而言,是运用自动化指挥控制系统将先进的侦察器材和远距离、高精度、大威力毁伤兵器融为一体的信息化武器系统。俄罗斯实施该计划的目的主要是为了在无力全面进行武器装备信息化建设的情况下,争取突出重点,在局部实现武器装备的信息化。英、德等国追随美军实施“横向技术一体化”计划的三项主要措施是:为现有主战装备加装数字化装置;使各武器系统实现“系统集成”;使火力打击兵器与C4ISR系统联网。

## 2.2 研制全新的信息化装备

西方发达国家凭借其强大的经济和科技实力,把发展新型信息化武器装备作为军队转型的重要内容。欧洲强国在发展信息时代的军事理论,特别是信息战理论,制定军队信息化长远发展构想的同时,积极研制新型信息化武器装备,用全新的设计思想和顶尖技术研发新装备,强化其探测、识别、打击、机动、定位和隐身等综合功能,增加武器库中的“新种群”,发展信息化作战能力和精确打击

能力。从20世纪90年代末开始,西方发达国家凭借其强大的经济和科技实力,把发展新型信息化武器装备作为军队转型的重要内容。到2030年前后,英法等国现役陆军主战装备将全部退役,不会再“修修补补”,而是采用全新的信息化装备和综合作战系统。

英、法根据美国“未来战斗系统”(FCS)概念,分别提出了发展陆军转型核心武器装备体系,即“未来快速奏效系统”(FRES)和“空地一体作战系统”(BOA)。FRES、BOA等项目涵盖了侦察监视、指挥控制、火力突击、火力支援、工程支援、后勤支援、通信、维修、医疗、核生化检测等几乎所有陆军作战功能,它们的共同特点是:在系统构成上都是由多种分系统组成,是模块化、通用化、网络化的“系统之系统”。法国陆军研制的“阿特拉斯”炮兵射击指挥系统V2版为全数字化的C4ISR系统,于2006年下半年交付使用,法国陆军的8个炮兵团和2个炮兵学校全部换此新装,从而大幅度提高其炮兵信息化作战能力。法国研制成功并已列装的“恺撒”榴弹炮系统和2R2M轮式迫击炮系统都配用了先进而复杂的一体化火控系统,信息化程度相当高。

俄罗斯的新军事装备技术发展步履蹒跚,它的新军事战略走向大体上与美国一致,但是总体上看俄罗斯的新军事战略尚未成型。尽管如此,从近几年俄罗斯的军队改革与拨款用途上看,俄军为了取得同美国等军事强国的新军事战略平衡,已经明确“精简兵员强化技术”的原则,制定了优先发展“全维优势”军事装备的目标。俄罗斯在新概念武器和炮兵C4ISR系统建设方面已经取得了很大的成绩,如炮兵部队装备了“饲养园”、“卷心菜虫”-B和“车辆”-M等自动化射击指挥系统和“成就”系列炮载自动化导引与火控系统以及120毫米“维娜”迫榴炮等,其轻型化、精确化、智能化程度都很高。俄罗斯已经研制出了世界上最先进的“布拉瓦”导弹武器系统(可携带10个分导核弹头,射程达8000公里),可用于装备海军及战略火箭部队,足以突破现有的任何导弹防御系统。

德国研制的“阿德勒”系统通过数传电台能够将炮兵的预警、侦察、指挥、控制系统和武器平台有机组成“一体化炮兵作战体系”。德国陆军目前正在研制新型软件对“阿德勒”系统进行改进,使其能够和陆军未来的指挥、控制和信息系统兼容。

德国正在的研制 155 毫米“聪明”灵巧炮弹完全属于新一代的信息化武器弹药。另外,德国、法国、英国和美国等还计划联合研制“炮兵系统协同作战”项目,以使各自的“阿德勒”、“阿特拉斯”、“贝茨”和“阿法兹”等炮兵指挥控制系统相互兼容。

瑞典研制的“阿莫斯”轮式迫击炮系统和 FH-77BD155 毫米车载式和轮式自行榴弹炮系统采用先进的一体化智能火控装置,信息化作战的能力很强,其精确度相当高,而外型趋于小型化,功效趋于智能化,携弹量增加,杀伤力与大型武器装备相当,且不受天候和战场条件制约,可对锁定目标实施全天候昼夜精确打击。另外,瑞典与法国正在联合研制“博尼斯”制导炮弹,意大利和荷兰正在联合研制“火山”155 毫米远程制导炮弹,这些信息化武器利用 GPS 导航技术为基础的弹道修正引信等信息化技术和装置将现役常规炮弹转化为“灵巧”炮弹,命中精度提高 3 倍以上,且一发弹道修正弹的价格仅为 2000~4000 美元。

### 3 对我军信息化的启示

90 年代的海湾战争以后,我国看到了高技术武器的重要性,逐步开始进行国家战略调整,加大军费投入,通过从俄罗斯,以色列等国引进了很多先进的军事技术,同时加大自主研发力度,在装备建设方面现已取得很大成果。

我国目前拥有比较完善的军事工业体系,虽然电子技术在某些方面和欧美相比稍逊,但是我国拥有较强的武器自主开发能力和武器整合仿制吸收能力。空间技术和导弹技术领先欧洲。军队在进行信息化建设的同时正迈向外层空间。但是中国的基础工业薄弱,工艺加工技术还有待提高,这些弱点直接影响中国武器的质量,寿命和出口。另外,我国需要加快民技军用步伐,使民用尖端技术第一时间转化到信息化装备创新和建设中。我们应顺应武器装备向信息化方向发展的历史性潮流,使武器系统大量采用信息技术,不断提高技术装备的信息化、智能化程度,使武器装备不仅具备应有的火力和动力,更具有信息力,即准确的侦察探测能力,实时的信息处理与传输能力,以及很好的隐身能力和远程精确打击能力。

### 3.1 加速升级现有武器装备及平台

采用“嫁接”和“贴花”使现有武器装备及平台快速升级,是我军装备信息化进程的第一步。例如,我国的单兵防空导弹世界先进,若在前期的 051 型、红箭级以及新型 022 级加装这种带有激光制导和光电瞄准的系统,防空能力将大大提高,而成本也不高。轰六换装新的飞行控制系统、雷达电子系统和使用新的空地武器后,旧貌换新颜,也能在未来的信息化战争中起到其应有的作用。

### 3.2 运用尖端信息技术综合集成武器系统

运用计算机和自动化控制等信息技术将相互独立的武器装备或设备综合集成成为新武器系统,是我军装备信息化进程的第二步。例如发展弹炮结合防空武器系统、机载高功率激光/高功率微波武器系统等,从而使武器装备或设备有效地综合集成。随着信息技术的发展,弹炮结合防空武器在作战时的效率比起单独使用导弹或高炮来说有着成倍提高,信息技术的发展,使得弹炮结合系统更加完美,作战将方式将由原来的人工控制转向智能化作战,自动接敌、识别目标、选择攻击武器都由雷达、火控等信息系统智能自动完成。这里的弹炮结合系统已经不再是原来意义上的便携式弹弹与小口径高炮了,老高炮与新导弹的整合如我国 57 高炮与 PL9 的结合将有更宽的发展之路。

### 3.3 发展我军的信息网络

未来战争是“网络中心战”,由此牵引着武器装备的发展。信息网络是“网络中心战”的基础,利用成熟的信息技术和共同的软件、标准及规范,实现不同武器系统之间的信息流动和共享,能够大幅提高其整体作战效能。各武器装备及平台的互联、互能、互操作是下一代军事指挥系统的基本要求;新型的六维空间战场建设(陆、海、空、天、电、心)是打赢未来信息化战争的必要条件;新出现的信息空间与信息共享空间是我们发展的重点;发展信息栅格、军事卫星和全维战场监视系统是重中之重。

我们的老式装备在火力与机动性上都还有很大的发挥余地,缺少的就是这种信息共享、资源共享能力。换装统一标准的数据链系统使各种装备之间形成信息共享、资源共享使各武器装备及作战平

台在作战的时候结束单打独斗的场面，进而真正做到体系与体系的对抗。

归根结底，我们要以科学发展观作为指导，立足于现实，立足于自身，加快实现武器装备跨越式发展。如果光靠买先进武器装备来实现信息化军事变革是不可能的，买的东西要么是赚技术，要么是救急。要实现武器装备跨越式发展，在构建信息化

军队建设和信息化作战的理论体系框架，建立以信息化作战牵动武器装备信息化建设的体制机制的同时，关键还要加大技术和人才投入，自主创新，研制生产和装备世界领先甚至超前的信息化武器系统，建立完备的信息化武器装备体系和各级军事信息系统。

## 参考文献（略）

## 作者联系方式

通信地址：北京怀柔 3380 信箱 13 号

邮政编码：101416

联系电话：010—66364289 13681131408

# 军队信息化发展战略之基本形势和战略方针目标

曹裕忠 林健

**摘 要:** 根据《2006—2020 年国家信息化发展战略》,结合我军新世纪新阶段历史使命和军队信息化发展的需求,本文阐述全球和我国军队信息化发展的基本形势,我国军队信息化发展的指导思想、战略方针和战略目标,试图为我国《2020 年前军队信息化发展战略》的研究论证提供粗浅的论点,而不提供相关论据。

**关键词:** 军队信息化; 发展战略; 基本形势; 战略方针; 战略目标

2006 年,中共中央办公厅、国务院办公厅印发的《2006—2020 年国家信息化发展战略》指出,“信息化是当今世界发展的大趋势,是推动经济社会变革的重要力量。<sup>[1]</sup>”同样,军队信息化是当今世界军事发展的大趋势,是推动新军事变革的重要力量。大力推进军队信息化,是覆盖国防和军队现代化建设全局的战略举措,是贯彻落实科学发展观、新时期军事战略思想和战略方针,全面建设信息化军队,实现武器装备的创新发展和信息战能力的跨越,以及努力做好军事斗争准备和打赢信息化战争的迫切需要和必然选择。

## 1 全球军队信息化发展的基本趋势

军队信息化是充分利用信息技术,开发利用信息资源,促进信息交流和知识共享,提高军队现代化建设质量,推动由机械化军队向信息化军队转型发展的历史进程。20 世纪 90 年代海湾战争以来,全球军队武器装备信息化与机械化建设相互交织、相互促进发展,推动军队管理体制的深化变革和军队编制结构的调整,重塑军事作战思想和作战理论。军事信息技术不断创新,武器装备信息化建设不断发展,信息化武器装备、军事信息系统和信息网络广泛应用,信息化成为全球军队信息化建设和发展的显著特征,信息化作战和网络化作战成为高技术条件下世界军事强国的主要作战样式,信息化战争和网络中心战成为世界军事强国的主要战争形态,并逐步向陆、海、空、天、电、网络、认知等全维、全域、全时作战方式演进。从“制陆权”、“制海权”、“制空权”发展到“制天权”、“制电磁权”和“制信息权”,使电子战扩展到“全频域、

全时域、全空域、能量域”的“制电磁权”斗争,而且谁掌握了信息优势制高点,谁就具有先敌作战的决策优势和行动优势,谁就能够取得战争的主动权,成为取得战争胜利的关键因素。军事信息资源与武器弹药资源、后勤保障资源一样日益成为现代战争无形的作战资源。军事信息系统是信息资源共享利用的主要平台。信息网络将更加普及并日趋融合,信息交流和知识共享将更加便利并日趋高效。战术互联网乃至全球信息栅格(GIG)为信息化作战的“物质流”和“能量流”提供了缩短从发现目标到实施精确打击时间的“信息流”。指挥信息系统在指挥控制、情报侦察、预警探测、通信导航、电子对抗、后勤支援等方面的作用日益显著。信息安全的威胁性和重要性与日俱增,成为各国军队面临的共同挑战。世界发达国家与发展中国家军队之间的数字鸿沟和信息不对称现象呈现扩大趋势,发展失衡现象日趋严重。发达国家军队信息化发展目标更加清晰,发展方向更加明确,投资力度更加集中,正在出现向信息化军队转型的趋向;越来越多的发展中国家军队主动迎接信息化发展带来的新机遇、新挑战,力争跟上世界新军事变革的时代潮流。因此,军队信息化将使现代战争形态发生重大变化,是世界新军事变革的核心内容;加快军队信息化建设和发展,已经成为世界各国军队的共同选择。

## 2 我国军队信息化发展的基本形势

### 2.1 军队信息化发展的进展情况

中央军委和总部一直高度重视军队信息化工

作。胡主席明确指出：将科学发展观贯彻落实到国防和军队建设中，必须着力推动军事理论创新、军事技术创新、军事组织体制创新和军事管理创新<sup>[2]</sup>。胡锦涛主席和军委、总部首长的指示对军队信息化建设的全面发展提出了明确要求，指明了发展方向；全军信息化工作领导小组对军队信息化发展重点进行了全面部署，做出了一系列重要决策；各军兵种从实际出发，认真贯彻落实，不断开拓进取，组织实施了一批军事信息系统和信息化武器装备重点工程，军事信息基础设施建设取得了长足进步，我军信息化建设取得了可喜的进展。可简要概括为：一是军队信息化理论创新成果层出不穷，有力地指导军队信息化建设；二是军事信息系统和网络实现跨越式发展，成为支撑军队信息化发展重要的基础设施；三是主战武器系统和装备信息技术含量不断提高，作战信息保障能力显著增强；四是军事信息技术在军队信息化建设各领域的应用效果日渐显著；五是指挥信息系统对提高信息作战指挥效率的作用日益显著；六是军事基础信息资源建设和开发利用水平不断提高；七是军事信息安全保障工作逐步得到加强；八是军队信息化基础工作进一步改善。

**军队信息化发展的基本经验是：**坚持站在国家安全战略高度，把大力推进军队信息化作为覆盖国防和军队现代化建设全局的战略举措，正确处理军队信息化与机械化之间的发展关系，长远规划，分步实施，持续推进。坚持从军情出发，因地制宜，把大力推进军队信息化作为解决复杂环境（尤其是复杂电磁环境）下一体化联合作战解决紧迫问题和发展难题的重要手段，充分发挥军事信息技术在各作战和保障领域的作用。坚持把开发利用军事信息资源放到重要位置，加强统筹协调，促进军事信息系统互联互通互操作和军事信息资源共享。坚持全面创新发展，加强军事需求、顶层设计和体制标准的综合论证研究，增强技术自主创新能力和系统综合集成创新能力，逐步增强信息化的自主装备能力。坚持推进军队信息化建设与保障军队信息安全并重，不断提高国防基础信息网络和军事信息系统的电磁安全防护和信息安全防护水平。坚持优先抓好军事信息化技术和装备的组织运用和作战运用以及技战术培训和作战训练，提高部队指战员军事信息技术应用技能和水平，提高部队在复杂电磁环境下信息化作战能力。

## 2.2 军队信息化发展中值得重视的问题

当前我国军队信息化发展也存在着一些亟待解决的问题，主要表现在：第一，需要进一步提高思想认识。我国军队是在半机械化和机械化建设不断加快、新军事变革和体制编制改革不断深化的条件下推进信息化的，军队信息化理论和战训实践还不够成熟，全军对推进信息化重要性、紧迫性的认识需要进一步提高。第二，军事作战需求研究不够清晰。军队信息化建设需求和高技术条件下联合作战需求研究的重任落在总部军事机关、军内科研单位和作战部队，但由于我国几十年处于和平时期，没有多少实际作战经验，因此军事需求研究仍然大多停留在以定性研究分析为主、定量分析为辅的局面，表述作战需求的各种能力难以细化和量化，军事作战需求分析研究和仿真验证能力急需增强。第三，需要进一步提高军事信息系统顶层设计能力。军事信息系统的体系结构、装备体制和技术体制论证水平和能力的提高，与军内科研单位研究论证的环境、手段、能力有关，与综合论证和联合论证的组织协调能力有关，关键是要提高指导军事信息系统和信息化武器系统等装备研制以及实现系统之间互联互通互操作能力，不然后期系统集成难以满足预期的作战需求。第四，要提高军事信息技术自主创新能力。研究和掌握一大批核心技术、核心器件、核心软件和关键装备是衡量军事信息技术自主创新能力的主要标志，依赖进口得不到核心技术，军工企业在技术预先研究和装备研制中的科技创新体系亟待完善，自主装备研发能力急需增强。第五，军事信息技术应用水平不高。在整体上，军事信息技术应用水平落后于实际军事需求，高新技术的军事应用潜能和作战运用效能尚未得到充分挖掘；在部分领域和军兵种军事信息技术应用效果不够明显。第六，要高度重视军事信息系统的信息安全防护问题。信息网络面临的计算机病毒、网络攻击、网络窃密、系统漏洞，以及电子通信系统面临的截获、侦察、干扰和电磁攻击等问题日渐突出，如应对不当，可能会对我军信息作战安全和国家安全带来严重影响。第七，军事信息系统的组织运用和训练效果不佳。军事信息系统的组织运用和作战运用研究的重任落在军内科研单位和作战部队，但由于构建大型模拟环境和训练环境（尤其是复杂电磁环境）的投资很大，技术复杂，满足联合作战要求的组织运用和作战运用的模拟和训练效果亟待提

高。第八,要加快军队信息化建设的体制机制改革进程。受各种因素制约,军队信息化管理体制尚不完善,业务归口管理机制尚不明晰或在调整之中,军事信息系统的技术体制和标准强制统一的进程需要进一步加快。

经过十多年的发展,我军信息化建设已具备了一定的基础,正处在由各系统独立建设,向整体建设、全面发展的过渡时期。客观上讲,我军信息化建设在各个领域已全面展开,通过狠抓顶层设计,强化法规标准,突出基础设施,注重重点突破,取得了初步成效。但从整体上看,我军信息化建设还处于全面发展的起始阶段,既要承接机械化军队的发展惯性,直面技术支撑相对不足、各种关系尚未理顺的现实,又要迎接发展需求不断加大、建设速度不断加快的巨大挑战。因此,这一发展时期是各种矛盾集中凸现期,信息化建设中各种深层次矛盾将会浮出水面。化解矛盾,理清思路,需要以科学发展观为指导,提高解决问题的针对性和实效性;抓住机遇,迎接挑战,需要更新发展理念,破解发展难题,创新发展模式,加快部队适应信息化作战的战斗力生成模式的转变。大力推进军队信息化发展,已成为我军履行新世纪新阶段历史使命重要而紧迫的战略任务<sup>[1][3]</sup>。

### 3 我国军队信息化发展的指导思想、战略方针和战略目标建议

#### 3.1 指导思想和战略方针

军队信息化发展的指导思想应是:以国防和军队建设重要思想、新时期军事战略思想和战略方针为指导,按照胡主席“要适应建设创新型国家的要求,围绕建设信息化军队、打赢信息化战争的目标,进一步实施科技强军战略,依靠科技进步和创新,加大战斗力生成模式转变”的指示,认真贯彻落实科学发展观,坚持以军队信息化带动机械化、以机械化促进信息化,坚持以军事理论创新、军事技术创新、军事组织体制创新和军事管理创新为动力,大力推进军队信息化,充分发挥军队信息化在加速推进战斗力生成模式转变发展中的重要作用,不断提高军队信息化水平,实现国防和军队建设又好又快地发展。

军队信息化发展的战略方针应是:统筹规划、

资源共享,面向战场、立足创新,深化应用、务求实效,军民结合、安全可靠。一是要以科学发展观为统领,以军事信息技术为主导,以科技创新发展为动力,坚持走机械化信息化复合发展之路,促进军事信息网络融合和新老装备信息融合,努力实现网络、应用、技术和装备协调发展,科学组织和有效利用军事信息资源,实现资源优化配置和信息共享。二是要以军事需求为牵引,以复杂电磁环境为背景,加强军事信息系统顶层设计、综合论证和军事信息技术应用研究,提高信息化武器装备组织运用和作战运用能力,加速建立完善军工企业科技创新体系,增强信息技术和装备自主创新能力,努力破解武器装备战斗力生成的难题,实现战斗力生成模式的转变,提升一体化联合作战综合保障能力。三是要把军事组织体制创新、军事管理创新与军事理论创新、军事技术创新放在同等重要的位置,完善体制机制,建立完善武器装备建设的竞争、评价、监督和激励机制,推动原始创新,加强集成创新,增强引进消化吸收再创新能力,提高打赢信息化战争的组织保证能力。四是要推动军民结合,协调发展,积极利用国家信息化技术、资源,建立平战结合、优势互补、安全可靠的信息系统和信息网络,提高信息化战争的战时综合保障能力。五是要高度重视电磁安全防护和信息安全防护,正确处理安全与发展之间的关系,以安全促发展,以安全保战斗力、保打赢,在发展中求安全,实现又好又快发展。

#### 3.2 战略目标

到 2020 年,军队信息化发展的战略目标应是:满足一体化联合作战需要的陆海空天基综合军事信息基础设施基本建立,军事信息技术和装备自主创新能力显著增强,集指挥控制、情报侦察、预警探测、通信导航、电子对抗、后勤支援等一体的军事信息系统体系结构完善、互联互通互操作能力显著增强,军事信息资源开发利用、优化配置和信息共享能力显著增强,复杂电磁环境下联合作战电磁频谱运用和管控能力显著增强,军队电磁安全防护和信息安全防护能力显著增强,军事信息技术应用能力和信息化作战能力显著增强,军队信息化发展的制度环境和政策体系基本完善,基本实现军队机械化向信息化转型,为迈向信息化军队奠定坚实基础。具体目标应主要有:



加速推进战斗力生成模式转变。围绕建设信息化军队、打赢信息化战争的战略目标,广泛应用信息技术,大力改造和提升机械化装备和机械化军队的信息化水平,推动战斗力生成模式转变的战略性调整;深化应用信息技术,加强信息系统的综合集成,努力解决“信息孤岛”,实现军事信息系统和信息网络的互联互通互操作;充分应用信息技术,进一步实施科技强军战略,依靠科技进步和创新,大力建设一体化的、综合的军事信息基础设施和军事信息系统,提高军队信息化建设的质量和效益。

实现军事信息技术自主创新、信息化装备发展的跨越。有效利用国家信息技术和资源,增强对引进技术和装备的消化吸收,突破一批关键技术,掌握一批核心技术、器件和软件系统,实现军事信息技术和装备从跟踪、引进到自主创新的跨越,实现军事信息系统和信息化武器装备由大到强的跨越。

提升军事信息网络建设水平、信息资源开发利用水平和信息安全保障水平。抓住网络技术转型发展的机遇,基本建成国际领先、多网融合、安全可靠的、满足一体化联合作战需要的陆海空天基综合军事信息基础设施。确立科学的信息资源观,把信息资源提升到与武器弹药资源、后勤保障资源同等重要的地位,甚至更加优先的地位,为提升武器精确打击、武器精确保障能力创造条件。信息安全的

长效机制基本形成,军队信息安全保障体系较为完善,电磁安全防护和信息安全防护能力显著增强。

增强中国特色的军事变革能力和军事信息技术应用能力。军事理论创新、军事技术创新、军事组织体制创新与军事管理创新能力显著增强,军队信息化发展的制度环境和政策体系基本完善,国防和军队信息化建设取得重大进展;广大部队指战员在复杂电磁环境下联合作战训练技能和军事信息技术应用技能显著提高,信息化条件下的防卫作战能力和信息作战能力显著增强,为建设信息化军队奠定基础。

## 4 结束语

我国军队信息化发展战略是国家信息化发展战略的重要组成部分,应根据国家信息化发展战略、全球军队信息化发展的基本趋势和我军信息化发展的基本形势,加大研究论证力度,适时提出并逐步修订完善符合我国国情、军情的军队信息化发展的指导思想、战略方针、战略目标、战略重点、战略行动和保障措施。以上观点仅供相关研究论证时参考。

## 参考文献

- [1] 中共中央办公厅、国务院办公厅印发《2006—2020年国家信息化发展战略》,2006年5月
- [2] 戴清民,“以科学发展观为指导,推进军队信息化建设的全面创新”,《军队指挥自动化》,2006(6)
- [3] 戴清民,“对军队信息化建设规律进行再认识”,《解放军报》(6),2007年2月13日

## 作者联系方式

通信地址:南京市后标营18号总参第六十三研究所

邮政编码:210007

联系电话:025-80827005

# 我军信息化建设的战略思考

鲍国民 聂建平 韩柯

**摘 要：**目前摆在我军面前的首要问题是军队信息化建设问题，这一问题将直接关系到军队建设大局。本文从军队信息化建设的战略意义、任务、目标、原则等方面进行论述，提出了一些基本方法。

**关键词：**军队；信息化；任务；目标；原则

高新技术的广泛应用，掀起了世界范围的新军事革命，信息技术成为这场新军事革命的核心。加速推进中国特色的军事变革，建设信息化军队，打赢信息化战争是我军的历史使命，研究这一问题有着重大的现实意义。

## 1 我军信息化建设的战略意义

军队信息化建设是以信息技术为基础，对军队建设的各个方面、各个环节进行信息化改造，实现军事指挥和控制的自动化，以提高军队的战斗力。军队信息化建设是建设信息化军队的过程，信息化军队是军队信息化建设的最终结果。信息化军队，是信息时代的重要军队形态，是由新型军事人员构成，以信息力为作战力，适于打信息化战争的网络化、知识化、一体化武装集团。加快军队的信息化建设，有着深远的历史意义和重大现实意义。

### 1.1 军队信息化建设是适应世界新军事革命的要求

进入 20 世纪 90 年代，新军事革命在广度和深度上有了新的发展，军队信息化的程度决定了其战斗力的强弱，成为决定战争胜负的关键因素。美、英、法、德等国已经启动新军事革命，在更多的军事领域开始进行“跨时代变革”，如进行训练革命、后勤革命等。工业时代的机械化军事形态更加深入地向信息时代的信息化军事形态发展，各国的机械化装备不断向信息化装备过渡，机械化战争加速向信息战争转变。美国投巨资为军队信息化进行基础建设，20 世纪 80 年代仅用于指挥自动化系统建设的经费累计超过 3000 亿美元，90 年代用于此

项建设的经费每年都保持在 4000 亿美元以上。近 10 年来，日本每年在指挥自动化系统这一项的资金投入约在 10 至 15 亿美元。印度军队的武器装备经费计划到 2010 年提高到 1300 亿美元，用于军队信息化建设的经费将大大增加。我国军队信息化建设刚刚起步，与世界军事强国的差距很大。只有顺应世界新军事变革的历史潮流、加强军队信息化建设，才能打赢信息化条件下的局部战争，保卫国家安全和国土的完整。加快军队的信息化建设成为我国军队一项紧迫的任务，也成为我国国防现代化建设的战略选择。

### 1.2 军队信息化建设是缩小同发达国家“军事技术差”的要求

“军事技术差”是指我国与重要军事强国在军事上的差距。这主要是指我国与发达国家在军事形态上所存在的差距，即武器装备、后勤保障及技术手段上的差距。从海湾战争看，美英联军的作战机器已经信息化，导弹发射、飞机出动、战场通讯、情报收集及军力调动等完全由计算机系统控制，而伊拉克军队则根本无法与其抗衡。目前，世界各主要军事强国军队的作战能力已达到信息化战争初级阶段的水平，而我国军队总体上，仍处于机械化阶段，信息化建设刚刚起步。

为了缩小同发达国家的“军事技术差”，我国在军队信息化和国防信息化建设上必须进行跨越式发展。

### 1.3 军队信息化建设是保卫国家安全和国土完整的要求

目前，国际上强权政治盛行，国际局势动荡不

安,我国的周边地区也不安定。为了维护世界和平及我国周边的局势,为了保卫改革开放的大好形势,使我国的经济有一个良好的国际环境,就必须建立强大的信息化、现代化的军队。

加强军事斗争准备,准备打赢一场高强度的局部战争,保卫祖国统一和领土完整,是我军肩负的神圣而又艰巨的历史使命。为了保卫祖国的领土完整,我军必须在机械化尚未完成的形势下,快速完成信息化建设,缩小与西方军事强国的“军事技术差”。

## 2 关于军队信息化建设的任务

军队信息化建设任务是着眼现实和未来军事信息对抗需要,提升军队信息化作战能力。

### 2.1 研究军队信息化建设理论

军队信息化建设理论主要由基础理论、方法理论和发展理论三大部分组成统一的理论体系。基础理论是从理论层面分析、阐释并揭示军队信息化建设的理论,主要包括:军队信息化建设的有关概念及其内涵;军队信息化建设的必要性、重要性和可行性;军队信息化建设的特点和规律;军队信息化建设面临的形势、任务和要求以及军队信息化建设中存在的矛盾及问题等等。方法理论是从实践层面回答并解决如何建设军队信息化的理论,主要包括:军队信息化建设的目标、指导思想、基本原则、手段方法和途径等。发展理论是从未来角度探索和展望军队信息化发展方向的理论,主要包括:军队信息化发展的前景预测、信息技术需求和信息化功能拓展等。对上述理论进行深入系统的研究,应当成为当前军队信息化建设发展中一项重要的理论建设任务。

### 2.2 制定军队信息化建设指标

军队信息化建设指标是衡量军队信息化建设发展质量的重要尺度和标准,由质量指标、技术指标和功能指标三大部分组成。质量指标是对军队信息化建设的质量规格和检验方法所制定的标准;技术指标是对军队信息化建设从技术文件上所做的若干技术规定;功能指标是对军队信息化建设提出的目标功能要求。

将制定统一的建设指标和规范作为一项信息化建设的重要任务,不仅可为军队信息化建设提供一种共同遵照的依据和内在的技术目标驱动力,而且对保证军队信息化建设质量、合理利用信息设备和资源、理顺建设关系以及提高建设效率均具有重要作用。

### 2.3 突破军队信息化建设的关键技术

军队信息化建设与发展有许多关键技术需要突破。从目前所掌握的国内外信息化发展情况看,军队信息化建设应优先突破的关键技术主要有以下五类:即战场数字化技术、指挥自动化技术、决策智能化技术、打击精确化技术和保障网络化技术等。在这几类关键技术之下,还有相应的若干具体支撑技术,即在军队信息化建设中,能够直接支持并满足军队信息化建设需求的技术,此类技术更多是一些基础性的信息化软件和信息化硬件等先进技术。对这些关键技术及核心技术的研究、开发和创新,已成为军队信息化建设的当务之急,一旦取得重大突破,军队信息化建设中的诸多理论问题和技术问题也就会迎刃而解。

## 3 关于军队信息化建设的目标

军队信息化建设的目标,是一个时期或一个阶段军队信息化建设发展追求达到的最高境界,也可理解为根据军队信息化建设的任务所提出的目的和标准。正确设定军队信息化建设目标,一是应深入分析建设环境,包括建设的内部环境和外部环境;二是应客观评估信息资源和潜力;三是应综合考虑信息科技水平;四是应科学论证军事需求;五是应优化选择目标实现的基本途径。军队信息化建设目标与建设实力之间始终是一对矛盾,军队信息化建设目标定的越高,要求建设实力越强,手段就越多,投入也越大。如果实力水平达不到,则必须调低军队信息化建设的目标,假若维持军队信息化建设的既定目标,那么必须要增加投入、增多手段,以确保目标与实力间的平衡和协调。根据我国军事、经济、科技和综合国力的情况,本世纪前叶军队信息化建设发展的基本目标,就是要突破和掌握军队信息化建设的关键技术,在现有武器装备率先实现信息化的基础上,将军队建设成为一支集战场

数字化、指挥自动化、决策智能化、打击精确化和保障网络化于一体,具有信息特色鲜明、网络系统优化、作战功能完备和天地信息融合的信息化战略导弹部队。

## 4 关于军队信息化建设的原则

军队信息化建设的原则,是军队在信息化建设中应当遵循的基本准则,是对军队信息化建设指导思想的具体体现。在军队信息化建设发展中,应遵循以下四条基本原则。

### 4.1 坚持需求牵动

坚持需求牵动,一方面,要正确预测军事领域信息化建设发展和变化情况。人类正在跨入信息化时代,未来军事对抗主要是在信息领域和空间领域进行的对抗,其作战样式、作战理论、作战方法和作战手段等都将会发生诸多重大变化,对于这些可能的变化,必须有一个清醒的认识和足够的估计,以使军队信息化的建设发展,始终能朝着未来打什么仗,信息化就怎么建的正确轨道上发展,以满足军队未来信息化威慑和信息化作战的需要。另一方面,要科学预见信息技术的未来发展。信息技术是飞速发展的技术,随着信息时代的发展,越来越多的新型信息技术和尖端技术也将不断涌现,对于此方面技术的未来发展,在军队信息化建设之初,也必须有一个科学的预见和超前技术准备,以保证军队信息化建设发展始终处于一种主动地位甚至领先的水平。

### 4.2 坚持技术创新

坚持技术创新,一是要有创新观念意识。观念意识对技术创新具有决定性的作用,有什么样的技术创新观念和意识,就有什么样的技术创新行为。二是要有创新的人才条件。人才是创新的根本,也是军队信息化技术理论创新的主动动力。三是要有创新的方法手段。应充分利用现代先进的计算机手段,通过虚拟现实、模拟仿真和演示验证等方法,论证并评估军队信息化建设理论的先进性、技术的可行性、方案的完备性和应用的效益性。

### 4.3 坚持重点发展

在硬件建设中,应以武器装备信息化建设为重点,以武器装备的信息化带动军队全面信息化建设;在软件建设中,应以信息处理软件和应用软件的研制为重点,突出指挥自动化和决策智能化软件系统的开发;在理论建设中,应以军队信息化的实施战略理论为重点,以宏观理论正确指导军队信息化建设;在技术建设中,应以信息共享技术的研发为重点,提高信息利用的效率。坚持重点建设和重点发展,不是忽视一般项目的建设,更不是取消或反对其他项目的建设,而主要是通过有重点的建设寻求突破口,以此带动一般项目乃至整个军队信息化建设的共同协调发展。

### 4.4 坚持“三个结合”

一是要平战结合,就是将军队信息化平时的战备建设与战时的应急建设相结合。军队信息化建设应以平时建设为主,以战时应急建设为辅,将军队信息化建设的功夫多下在平时,加大对平时建设的投入力度,增加平时建设的先进技术储备,努力克服“看中建建和建中看看”的不利倾向。二是要军民结合,就是在军队信息化的建设中,利用军地双方的信息资源,进行多元化结合性建设。军队信息化建设总体上应立足以自身建设为主,以地方协作建设为辅,这就要求军地双方从信息技术攻关、信息资源设备使用、信息模块部件生产和演示验证环境保障等多方面予以通力合作,以充分发挥军地两种力量在军队信息化建设中的互补优势,加速军队信息化建设的进程。三是要土洋结合,就是在军队信息化的关键技术及核心前沿技术的研究开发中,将国内与国外、自研与引进紧密结合起来,使之在军队信息化建设中得到有机地整合,要始终坚持走以我为主的自研开发建设之路,借鉴国外的先进技术应在消化的基础上加以吸收,所有的技术引进都必须能够为自主式技术研发服务,从根本上防止在军事信息技术发展中受制于人。

## 5 军队信息化建设应注重解决的问题

军队信息化建设是关系到军队长远建设发展的一件大事,也是我们当前一项刻不容缓的战略任务。为确保军队信息化建设在正确的轨道上持续、

稳定、健康、高效地发展，除了明确军队信息化建设的任务、目标和原则外，还要重点把握好以下几个问题：一是应下大力研究探讨军队信息化建设发展的有关理论问题，从建设理论、发展理论和应用理论三个方面进行深入系统的研究，逐步形成较为完善的军队信息化建设发展理论体系，为军队信息化建设与发展提供科学的理论依据；二是在认清军队信息化建设发展的特点和规律的基础上，应正视军队信息化建设中的矛盾和问题，找到制约军队信息化建设发展的原因及症结，提出解决军队信息化建设发展“瓶颈”问题的有效办法，同时还应严格按照军队信息化发展的规律指导战略导弹部队信息

化建设发展的实践；三是要妥善处理军队信息化建设发展与我国空间信息网建设之间的关系，使军队信息化建设与国家和军队空间信息网建设同步互动起来，在军队信息化建设中必须考虑对空间信息网资源的利用，在空间信息网的建设中也应有目的、有重点地考虑军队信息化建设的需求；四是应将我军特色贯穿于军队信息化建设的全过程，特别要注意突出军队建设的有效性和有效性建设问题，真正走出一条符合军队实际，能满足“多重威慑、多重作战”任务需要的“边建边用、边用边建、建用并举”的信息化建设发展新路。

### 参考文献

- [1] 丁锋.民技军用，功在千秋.军民两用技术与产品，2005
- [2] 刘朝勋，任希魁.论我国国防经济建设的跨越发展道路.理论月刊，2004
- [3] 《军队信息化建设》

### 作者联系方式

通信地址：武汉市解放公园路 45 号通信指挥学院研究生管理大队

邮政编码：430010

联系电话：010-80647689    010-66820275

# 信息化条件下维修保障建设构想

陈永龙 徐宗昌

**摘要：**我军装备跨越式发展离不开维修保障信息化的建设。提出了信息化条件下维修保障的定义和目标，指出维修保障信息化建设也要分“三步走”，要建立高效的领导机构；规划好装备采办、平时管理和战时指挥三个重要环节的信息链路，以实现维修保障的全过程优化；在维修保障所包含的管、修、供、训、战等专业领域以及各军兵种的维修保障方面实现一体化；同时要考虑维修保障装备的配套建设，将信息化的方法和技术应用到主战装备与保障装备的全系统建设中去。

**关键词：**军队信息化；装备维修保障；全过程优化；一体化；全系统建设

信息技术在军事领域的广泛应用，使军队的作战方式和作战手段发生了变化，必将对作为军队战斗力重要基础的装备维修保障产生巨大冲击，对其发展方向也将产生重大影响。信息化条件下维修保障（也称为维修保障信息化）建设具有战略性、长期性、整体性的特点，涉及到军队建设的方方面面，是一项长期而复杂的系统工程<sup>[1]</sup>。研究和探索信息化条件下的装备维修保障建设，对于增强信息化战场中的装备维修保障能力，保障信息化战争的胜利具有重要意义。

## 1 信息化条件下维修保障建设的定义与目标

信息化条件下维修保障是指在国家军事领导机关的统一规划和组织下，在装备维修保障领域应用现代信息技术，大力发展、使用信息化保障资源和深入开发、利用信息资源，加速实现装备维修保障现代化的进程。它是国防信息化和军队信息化的重要组成部分，同时还必须依托国家信息化、国防信息化和军队信息化建设。

由于信息化条件下维修保障建设是一个动态的发展过程，其建设目标将在信息化战争需求的牵引和现代信息技术发展的推动下，不断从低级向高级发展。当前，我们认为信息化条件下维修保障建设的目标是：广泛应用现代信息技术，实现与信息化装备发展及使用相适应的装备维修保障手段信息化和装备维修保障指挥与管理信息化，为未来信息化战争提供高效、精确、快速、及时的装备维修保障。为了实现这个目标，提出以下几个方面的建设构想。

## 2 制定长远性规划，建立统一的组织领导机构

### 2.1 信息化条件下的维修保障建设分“三步走”

中央军委科学地提出了今后五十年国防和军队现代化建设“三步走”战略构想。信息化条件下维修保障建设必须遵循“三步走”的发展战略，要瞄准信息化战争，做好长远性建设规划。同装备建设“三步走”的时间节点相对应，今后50年装备维修保障建设也应该划分成三个阶段。第一阶段是到2015年，针对重点领域和敏感区域建设功能完备的装备维修保障模式，形成装备维修保障信息化基本体系，具备遂行新时期军事斗争装备保障的信息化手段，满足现实军事斗争准备需求；第二阶段是到2025年，同装备建设步伐相协调，加速信息化条件下维修保障建设步伐，完善信息化体系，使装备保障能力有较大发展；第三阶段是到2050年，全面推进并基本实现装备维修保障信息化。

第一、二阶段，是初级阶段，要利用已有的信息基础设施，应用现代信息科学技术，深入开发和充分利用装备的订购、验收、储存、供应、管理、使用、维修、训练和报废等信息，做到指挥自动化、决策科学化、保障精确化，提高装备保障的时效性，增强装备维修保障能力，降低维修费用，不断促使装备维修保障的模式、方法和手段产生新的变革。第三阶段是高级阶段，要广泛采用信息产品或高技术产业的最新成果，以计算机网络技术和多

媒体通信技术为基础,将各级保障部门、各种保障单元和保障平台,以及地方保障力量都置于保障环境下的计算机网络中,形成协调一致的保障体系,高效运用维修保障力量,实现纵横结合、多边协作,使装备保障的时间、空间、数量、质量要求尽可能达到精确化的程度,最大限度地开发信息资源。

## 2.2 考虑全局性发展,建立统一的组织领导机构

为了实行集中统一的领导,搞好信息化条件下装备维修保障建设,应当成立一个高效、权威的领导管理机构——全军维修保障信息化领导小组,全盘筹划装备维修保障信息化建设进程,科学进行顶层设计工作,并确保规划的成果能够在全军范围内贯彻执行。该小组在“全军信息化工作办公室”的领导下,负责领导全军装备维修保障信息化建设工作,主要包括审查、颁布装备维修保障信息化的方针、政策、法规与标准,规划并领导实施全军装备维修保障信息化工程,以及组织重大关键技术项目的攻关等;在装备维修主管部门设立全军装备维修保障信息化办公室作为该领导小组的办事机构,负责处理日常事务的工作;各军兵种、各战区的装备部门也应当设立相应的领导与管理组织,领导所属部队的装备维修保障信息化工作。各级机构的建

立,是主动引领全军装备维修保障信息化建设,改变信息化过程中可能出现的无序状态,并将军队各级开发的信息系统纳入信息化轨道的最有效的方法,是装备维修保障信息化建设走上健康、有序、快速发展道路的重要保证。

## 3 立足全过程优化,规划畅通的保障信息链路

### 3.1 应用现代信息技术,实现武器装备采办与保障管理信息化

新研装备的寿命周期过程如图 1 所示,一般经历论证与方案、工程研制与定型、生产与部署、使用保障和退役等阶段,每个阶段都有相应的综合保障要求和相应的数据管理要求<sup>[2]</sup>。装备从论证到退役的整个寿命周期过程各阶段是互相关联的。根据全系统全寿命管理和并行设计的理念,从研制一开始就考虑保障问题,对装备系统的保障性与保障过程进行综合、并行的设计与研制,确保主装备与其保障系统同步研制,同时交付部队使用。可见,研制阶段的产品数据,将对装备的维修保障活动产生直接的影响。因此,必须采用有效的信息技术和手段对这些信息进行记录和管理。

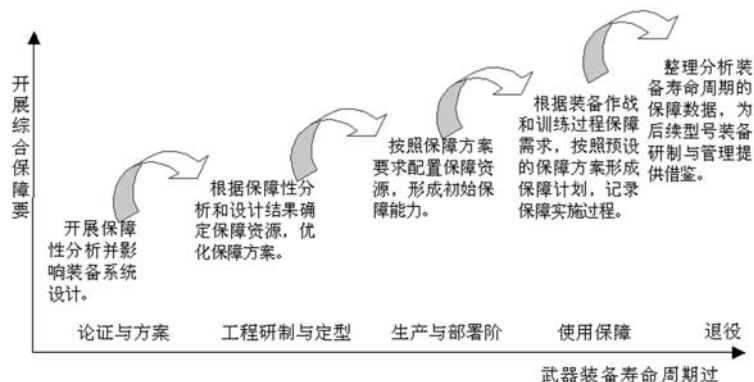


图1 武器装备寿命周期过程的综合保障要求

从 20 世纪 80 年代中期开始,美国防部开始推行一项设计、制造和后勤保障共用信息系统,称为“持续采办与寿命周期保障”(CALS)<sup>[3]</sup>。我军可借鉴美军的先进做法,高度重视装备采办过程中的信息数字化、标准化工作,通过制定和实施一系列的管理和控制方法,充分应用现代信息技术,实现

武器装备采办与保障管理的信息化。

### 3.2 建立装备维修保障信息管理系统,提高平时保障管理水平

装备维修保障平时管理、决策活动离不开信息工作,其工作水平受到信息化程度的影响和约束。

美军的维修保障信息管理系统,属于美军后勤管理系统,大多数建于20世纪70年代初期。随着信息技术的发展和武器装备保障的需求变化,20世纪80年代初对这些系统进行了大规模改造。目前美军在各军兵种总部和部队各级都建立了相应的保障信息系统,并不断进行充实和完善。这些信息系统的开发为实时掌握装备动态信息、科学决策提供了信息支持。我军各军兵种也相继开发了适应各自特点需要的、用于装备维修保障管理的业务信息系统,有效地促进了装备维修保障管理、决策效能的提高。但是,这些系统功能不一,数据格式不同,难以实现不同系统之间的互连互通互操作,必须着眼全寿命保障的信息要求,统一规划开发完善装备维修保障管理信息系统。该系统要具备信息收集、信息传递、信息处理、信息显示及辅助决策等基本功能。

### 3.3 开发装备维修保障指控系统,提高战时保障活动的精确度

信息化条件下的高技术战争,装备作战效能的发挥和战争的胜利更加依赖于精确、敏捷、高效的维修保障。要改变原有的技术保障模式,变被动反应式保障为主动预见性保障,这就要求充分利用信息优势,随时了解和掌握战场变化形势,提前预知作战部队的维修保障的需求,从而保证技术保障系统适时地供应保障资源和提供装备保障能力。而获取、处理各类数据和通信系统的关键是开发各种装备维修保障指控系统。指控系统在集成数据环境下,通过战时维修保障信息网络,可以随时掌握参战装备和后备装备的数量、技术状况、战斗损伤、故障修理与战场抢修、战备器材供应、战场抢修力量与调配等方面的动态信息,利用这些信息,可以实现资源可视化和战场可视化。指挥员可以准确把握战场维修保障的全局,并通过信息网快速、及时地下达维修保障指令,以最短时间调配维修保障资源,组织战场抢修,实现精确、敏捷的技术保障。

另外,装备采办、平时管理和战时指挥三个不同阶段之间所拥有的信息不是相互独立的,而是密切相联系的。装备维修保障信息化建设必须从全寿命的观点出发,全面考虑和设计信息管理的功能与数据元素,确保形成的信息资源能够得到有效的利用。

## 4 着眼信息化战争,建设一体化信息体系结构

### 4.1 加强各保障专业的一体化建设

为了加速维修保障由机械化向信息化的转变,在各军兵种装备维修保障信息化建设过程中,除了要从装备全系统、全寿命信息管理出发,解决装备维修与订购、验收、培训、储存、供应、运输、使用等其他装备保障工作及其信息的综合与集成,形成共享的集成数据环境外,特别要在装备的管、修、供、训、战等专业工作方面加强研究和建设,实现数据格式的统一、信息资源的共享和信息平台的交互。为此,装备维修保障信息化建设要着重实现多专业的集成,将传统的装备管、修、供、训、战等环境在信息层面上紧密结合,实现一体化的信息系统体系结构,使信息能够共享。

### 4.2 谋求各军兵种维修保障的一体化联合

为了适应信息化条件下一体化联合作战的维修保障需求,在对装备进行系列化、通用化、组合化设计和建设多任务、多功能的武器装备体系与作战平台的基础上,首先要谋求各军兵种维修保障向联合模式转变,实现维修保障力量一体化。为此,要建立一体化、分布式保障体系,将各军兵种独立的保障机构转变为一种分布式的、联合的基础设施,实现维修保障资源一体化联合配置;要建立各军种通用的一体化保障信息系统和连接所有地方企业的信息系统,建立强大的运输网络和物资器材可视化系统,实现信息资源的融合与共享;用“保障速度”取代“保障规模”,实现各军兵种维修保障的一体化联合。

### 4.3 重视装备维修保障底层信息的一体化研究

为了实现维修保障信息系统的互连互通,减少不必要的浪费,要重视信息化基础工程建设。这方面可借鉴美军的JTA的思路,为信息系统开发建立统一的技术体系结构与标准。同时,可借鉴美军开发GCSS系统和我国交通部开发ITS系统的经验,在顶层设计的基础上,将信息系统共同的部分进行封装,建立通用的装备维修管理信息系统开发平台,给各单位开发人员提供半成品的软件框架<sup>[4]</sup>。



这样不仅减轻了开发人员的工作量,也可以保证全军装备维修保障信息系统更好实现集成,保证信息化建设的持续性和先进性,不断推进信息化体系的配套建设。

## 5 适应主装备发展,同步配套地发展保障装备

保障装备是武器装备维修保障的重要手段,是保持和恢复军队战斗力、实现保障有力的物质基础。随着信息技术的快速发展与广泛应用,维修保障装备的发展也面临着一些新的挑战 and 任务。要按照综合保障思想,在装备研制初期就开始考虑保障问题,即尽早规划和研制配套的保障装备,以便在装备部署时能够及时地建成经济有效的保障系统,从而以最低的寿命周期费用提供所需的保障<sup>[5]</sup>。随着武器装备的发展,装备本身的信息化程度越来越高,如果没有配套的信息化保障装备,武器装备的维修保障将异常艰难。因此,装备维修保障信息化建设必须要延伸到武器装备的研制初期,要结合新装备的建设,同步研制信息化保障装备。要将信息化保障装备列入武器装备体系,做到同步规划与计划、同步论证与研制、同步生产与部署。在研制与

生产信息化装备和信息化保障装备时,采用并行工程、保障性工程方法,以及 CALS、“基于仿真的采办(SBA)”等信息化的方法。在装备使用试验时,及时提供信息化保障装备进行相关的保障性试验。在装备部署使用时,将信息化保障装备作为配套的保障资源同时交付部队使用,达到全过程建设的目的。对于现役装备进行信息化改造时,应同时提出维修保障装备的信息化改造,并使两者同步、协调地进行。

## 6 结束语

最近发生的几场局部战争的实践表明,随着大量高技术装备与信息化装备的投入使用,装备战损率明显增高、维修保障难度加大、任务更加繁重,良好的维修保障成为提高装备战斗力的倍增器,是发挥装备作战效能,乃至决定战争胜负的重要因素<sup>[6]</sup>。因此,要充分认识装备维修保障在现代战争中重要地位与作用,把维修保障建设提高到与新装备建设和作战指挥同等重要地位来对待,加大装备维修保障信息化建设的力度,将以上构想逐步变成现实。

### 参考文献

- [1] 杨学强,黄俊.装备保障信息化[M].北京:装甲兵工程学院,2006
- [2] 徐宗昌.保障性工程[M].北京:兵器工业出版社,2002
- [3] 徐宗昌.装备保障性工程与管理[M].北京:国防工业出版社,2006
- [4] 宋建社,曹小平.装备维修信息化工程[M].北京:国防工业出版社,2005
- [5] 单志伟.装备综合保障工程[M].北京:国防工业出版社,2007
- [6] 总装备部综合计划部.信息化战争装备维修保障[M].北京:国防工业出版社,2007

### 作者联系方式

通信地址:北京市丰台区杜家坎21号装甲兵工程学院技术保障工程系

邮政编码:100072

联系电话:010-66718948-803 13521120538

# 军用共性软件体系结构研究展望

初宁 曲向丽 李雪娇 姜峰

**摘 要:** 本文着眼于未来网络中心战环境对军用共性软件的发展要求,对其体系结构研究的军事需求进行分析,并对该项研究的几个重要方向进行了展望。

**关键词:** 军用共性软件; 体系结构; 网络中心战

## 1 引言

软件体系结构 (Software Architecture, 简称 SA) 是控制软件复杂性、提高软件系统质量、支持软件开发和复用的重要手段之一,自提出以来,日益受到软件研究者和实践者的关注,并发展成为软件工程的一个重要的研究领域<sup>[1]</sup>。

军用软件包括军用共性软件和专用软件。军用共性软件提供公共支撑服务,专用软件提供各种专用服务,并在共性软件的支撑下完成专门的军事使命。

军用共性软件是信息化武器装备的核心和灵魂,在武器装备信息化建设中具有核心地位和关键作用。“十五”期间,军用共性软件的研制主要针对指挥信息系统的共性应用技术,在软件集成框架、数据集成框架、联合指挥作业框架、战场情况综合框架、通用传输服务框架、共性应用支撑软件、共用业务软件和共用技术保障软件几个方面展开,它们相对分散、孤立,缺乏从体系结构层面展开的整体分析、设计、描述和评估,这对于军用共性软件从单纯的指挥领域全面走向全军各级各类信息应用领域构成了制约。为适应未来网络中心战的需要,对军用共性软件的体系结构进行充分研究已经成为一个必须。

## 2 军事需求分析

具体说来,对军用共性软件体系结构的研究可满足如下军事需求。

1) 适应未来网络中心战环境,实现各级各类军事信息系统灵活、动态、无缝链接的需要。

未来的网络中心战,其实质是在武器装备信息

化的基础上,利用通信网络将分布在广域环境内的各种传感器、指挥中心、业务中心和各种武器平台连接成为一个统一高效的有机整体,实现战场态势和武器的共享,把信息优势变为作战行动优势,使得主战部队、友邻部队和后备部队共同感知战场态势,从而协调行动,实现一体化联合作战,发挥最大作战效能。在这种战争模式下,各级各类军事信息系统之间的互联互通互操作成为一个必然要求。要实现它们之间的灵活、动态、无缝对接,作为军用软件公共支撑服务的提供者,军事信息基础设施的核心环节,军用共性软件的作用至关重要。必须从顶层对其体系结构加以研究,以应对这种复杂系统较链的需要。

2) 提高军事信息系统可用性、可靠性、安全性、可伸缩性、可扩展性、抗毁性,获取信息优势,形成知识优势和决策优势的需要。

软件体系结构的优良与否,直接关系到软件系统的质量。军用软件特殊的应用环境和实现目标要求军用软件应具有良好的质量特性,不仅要具有良好的性能表现,还应该具有高可用性、高可靠性、硬安全性、强可伸缩性和可扩展性,以及良好的抗破坏、抗摧毁能力,这些特性需要从体系结构这一基础层面提供根本支撑。

3) 强化我军信息系统顶层设计,提高军用软件开发效率,避免重复研制、盲目开发的需要。

军用共性软件是我军各级各类信息系统的底层支撑,对其体系结构加以研究,将会大大强化军用信息系统的顶层设计,渗透到整个军用软件系统的各个层面。

软件体系结构是对软件系统的高层抽象,位于整个软件生命周期的最初,设计优质的软件体系结构可以减少和避免软件错误的产生和维护阶段的高昂代价。对基于军用共性软件体系结构的软件开发

方法进行研究,可以为军用专用软件的研制提供基础性指导,降低软件开发复杂度,促进军用软件系列化、标准化、集约化生产。

### 3 研究要素展望

1) 军用共性软件的范围界定,及其功能性和非功能性特点分析。

军用软件包括军用共性软件和专用软件。军用共性软件是为全军各级各类信息系统提供基础支撑和共性功能的软件集合,具有特定于应用领域的功能性和非功能性特点。了解我军现有信息系统的实际情况,收集未来网络中心战环境下对信息化武器装备体系的需求,鉴别带有共性的支撑服务和各军兵种专用功能,合理规划共性软件的边界,明确性能指标要求,梳理分析共性软件的数据模型、信息模型以及流程模型,将是进行军用共性软件体系结构研究的第一步。

2) 面向军用共性软件体系结构模型的描述方法研究。

综合现有软件体系结构的模型描述技术,对比研究各项形式化描述语言以及图形描述方式的适用性,突出军事需求背景和共性应用要求,立足系统设计阶段需求,跟踪体系结构模型描述技术的发展前沿,确定适合新型军用共性软件体系结构的模型描述方法。

3) 面向未来网络计算环境的军用共性软件体系结构设计。

当前军用软件系统所基于的计算机硬件平台正经历从集中封闭的计算平台向开放互连的网络平台的转变,随着软件运行环境的演变,软件体系结构必然要进行相应的变革,这一步将首先从共性软件体系结构的变革迈出。目前,面向网络的计算环境正由 Client/Server 发展为 Client/Cluster,并正朝着 Client/Network 和 Client/Virtual Environment 的方向发展。而以软件构件等技术支持的软件实体将以多种形态存在于网络中各个节点之上,任何一个软件实体可通过某种方式加以发布,并以各种协同方式与其他软件实体进行跨网络的互连、互通、协作和联盟。对军用共性软件体系结构的设计应主要针对网络计算环境的异构性、动态性以及协同性进行,明确军用共性软件对外提供的接口,共性软件的内联关系,共性软件的战技战术指标等内容,使其能

够屏蔽软件实体的多态存在,支持多实体协同的灵活构建,感知外部网络环境的动态变化,并随着这种变化按照功能指标、性能指标和可信性指标等进行静态调整和动态演化。

4) 基于军用共性软件体系结构的军用软件开发方法研究。

由于所基于的平台是封闭静态框架,传统军用软件系统的开发基本都是采用自顶向下的途径,确定系统的范围总是建立需求的第一步,然后通过分解而实施分而治之的策略,整个开发过程处于有序控制之下。而适应未来网络计算环境的软件系统的开发所基于的平台是一个有丰富基础软件资源但同时又是开放、动态和多变的框架,开发活动呈现为通过基础软件资源组合为基本系统,然后经历由“无序”到“有序”的往复循环过程,基本上是一种自底向上、由内向外的螺旋方式。另一方面,在静态和封闭的环境下,传统软件开发方法和技术并没有将对软件的可信性(安全性和可靠性)考虑融合在其中,从而致使在网络环境下开发软件系统时,缺乏可以保证系统可信性的有效手段。对新型军用共性软件体系结构的研究,应着眼于未来网络计算环境,跟踪当前“面向服务”、“面向方面”等新兴编程模式,分析我军传统软件开发模式的优劣势,跟踪从体系结构到具体实现的映射技术,对基于军用共性软件体系结构的军用软件开发方法进行研究,以期达到提高我军软件系统研制效率、降低系统复杂度和风险度的目的。

5) 面向特定军事应用领域的共性软件体系结构研究。

特定军事领域的应用具有更加紧凑、更具针对性的共性软件系统,如能对其体系结构加以严格设计,并将直觉成分减少到最低程度,可以有效实现复用,提升体系结构的实际效能,并可借鉴领域中已经成熟的体系结构。譬如可以针对军用嵌入式系统领域,研究特定的共性软件体系结构,满足嵌入式系统之间、嵌入式系统和其他系统之间的信息共享要求,为一体化联合作战提供有力保障。

6) 对可靠性、安全性、可伸缩性、可扩展性、抗毁性、易用性、易维护性加以统筹考虑,强化支撑的软件体系结构设计。

军用软件的应用背景决定了军用软件必需提供具有相当可靠性、安全性、可伸缩性、可扩展性、抗毁性、易用性以及易维护的能力。作为军用软件

背板的共性软件，在其体系结构设计最初，就必须将这些要素进行统一考虑，集中规划，而不能采取亡羊补牢的做法。

7) 基于军用共性软件体系结构的计算模式、编程模式研究。

新的软件体系结构需要新的计算模式和编程模式支撑。只有对计算模式和编程模式进行针对性研究，才会将体系结构的研究成果落到实处，指导军

用软件的研制，真正发挥新型体系结构的效能。

## 4 总结

本文对军用共性软件体系结构研究的军事需求进行了分析，并对其研究要素加以了展望，以适应未来网络中心战环境下的军用软件发展需求。

## 参考文献

- [1] 梅宏，申峻嵘，软件体系结构研究进展，《软件学报》Vol.17， No.6， June 2006， pp.1257—1275

## 作者联系方式

通信地址：北京市丰台区大成路 13 号 R02

邮政编码：100039

联系电话：13911132183 010-66820294

# 网络中心环境中C<sup>4</sup>ISR作战视图产品描述

邓鹏华 毕义明 刘顺成

**摘 要:** C<sup>4</sup>ISR 视图产品描述是 C<sup>4</sup>ISR 系统开发的基础。为支持网络中心战能力, C<sup>4</sup>ISR 体系结构框架必须进行完善以适应网络中心环境 (Net-Centric Environment, NCE)。通过对 NCE 中 C<sup>4</sup>ISR 作战视图 (Operation View, OV) 产品的描述, 可为从军事人员的视角对开发先进、互操作的、综合集成的、支持网络中心能力的 C<sup>4</sup>ISR 系统提供指导。

**关键词:** 网络中心环境; 作战视图; 产品描述

## 1 引言

体系结构是指“组件的结构及其关系, 以及支配它们设计和随时间演化的准则和指导方针”<sup>[1]</sup>。体系结构描述是对现实或构想的现实世界资源、规则和关系的配置的表示。一旦这种表示进入系统开发生命周期过程中的设计、开发和采办阶段, 体系结构描述转变成为战场中能力和优势的实现。而体系结构描述则由视图内或视图间相互作用的体系结构产品组成。

C<sup>4</sup>ISR 体系结构框架为体系结构描述提供了规范化途径和方法, 对体系结构的理解、比较和集成建立了共同的标准, 从而有助于建立各军种、各部门间可互操作的、最佳费效比的 C<sup>4</sup>ISR 系统。

美国自 1996 年 7 月颁布了《C<sup>4</sup>ISR 体系结构框架 1.0》<sup>[2]</sup>后, 一直致力于体系结构框架标准的制定<sup>[1][3][4]</sup>, 目前最新版本为今年 4 月份的《国防部体系结构框架 1.5》<sup>[4]</sup>。这个文件的最大特色之一就是增加了在 NCE 中体系结构产品的描述, 它充分反映了信息技术快速发展对军事理论、作战方式的改变, 体现了美国军方正在向一种新的信息密集型作战——网络中心战 (Net-Centric Warfare) 的转型——这种转型毫无疑问将直接影响 C<sup>4</sup>ISR 系统的设计与开发。

本文介绍了文献[4]中对 NCE 中的作战视图产品描述, 它反映了军事人员对系统的功能 (能力) 需要, 方便了军事人员在系统设计阶段对系统的理解、比较和审查, 可为军事人员参与开发支持网络中心能力的 C<sup>4</sup>ISR 系统提供指导。

## 2 网络中心战与网络中心环境

“网络中心战”是描述信息时代如何进行组织和作战的最佳术语, 它通过将传感器、决策者和发射装置组网, 实现感知共享、增大指挥速度、加快作战节奏、增大杀伤能力、提高生存能力, 并实现一定程度的自同步, 从而增强作战能力。网络中心战本质上是通过有效联接有识实体, 将信息优势转化为战斗力<sup>[5]</sup>。

网络中心环境 (NCE) 是指网络中心战存在的作战环境的状态和特征。即各作战节点间通过网络化实现实时或近实时的信息共享, “鲁棒”的传感器网络产生了共享感知和高质量的信息并能随时随地按需传送到需要的节点上, 并通过指挥控制使作战部队协同作战并最终实现自同步。

在这种情况下, C<sup>4</sup>SIR 系统需要进行演化以适应 NCE 中决策的日益增长的需求, 从而促进网络中心能力的开发, 充分将信息优势转化为战场优势。

## 3 NCE中C<sup>4</sup>ISR作战视图产品描述

NCE 中的 C<sup>4</sup>ISR 体系结构具有融为一体的作战视图 (OV)、系统与服务视图 (SV)、技术标准视图 (TV) 和全视图 (AV)。这些视图保证了在各个军种以及其他使用者之间的互联、互通、互操作, 避免“烟囱”式 C<sup>4</sup>ISR 的产生, 充分支持网络中心能力。体系结构的各个视图之间相互联系并在整体上表示了体系结构。

其中 OV 包括作战节点、节点执行的任务或活动和为完成使命而必须交换的信息。它体现的是军事人员的视角,关注于为执行特定使命或任务而具备的能力(功能)以及执行过程中所需的信息流。 $C^4ISR$  体系结构作战视图共有七种产品。下面将依次介绍。

### 3.1 高层作战概念图(OV-1)

在 NCE 中,OV-1 以附有文本(一个或多个)的图形形式提供了使命的高层图形视图,描述了体系结构包括的网络中心能力、所属体系结构的范围和支持使命的网络中心作战角色,以及  $C^4ISR$  体系结构如何利用完全网络化的环境和集成方法完成使命。它的一个重要方面是对可靠的、可见的信息和能力的描述。OV-1 说明了体系结构应该“做什么,怎么做”。

### 3.2 作战节点联接描述(OV-2)

NCE 中的 OV-2 用来以图形形式(如 UML 协作图或结构化图)确定已经指派作战角色(如服务功能提供者,服务使用者和未可预料的潜在用户)的作战节点间的信息交换需要,它反映了信息共享的需求,而这种需求通过需求线(needline)来表示。需求线用箭头表示,表明了信息流的方向。它只表明信息转换需求而不关注于信息转换是如何进行的,如在节点 A 产生的信息通过节点 B 传送到节点 C 使用,则节点 B 并不出现在 OV-2 图中,即每个箭头只表示在两个关联的节点之间存在某种信息迁移的需求。

作战节点的角色中,服务功能提供者是服务(信息和能力)的提供来源,它必须确保服务时刻是可使用的,并且必须考虑未可预知的用户。服务使用者通过获得的服务来履行使命,而未可预知的潜在用户代表了信息时代作战人员的动态、即时的需求,网络中心 OV-2 必须描述未可预知用户能够在 NCE 中发掘信息和能力以支持其使命的变化的、难以预知的需求。

### 3.3 作战信息交换矩阵(OV-3)

在 NCE 中 OV-3 获取确定网络中心方式获得或提供的信息所需的指导方针,它确定信息元素和信息交换的相关属性,将信息交换与产生或使用信息

的节点及交换对应的需求线联系起来,描述了用 OV-2 中需求线表示的信息交换的细节(一个需求线可以与多个信息交换相对应)。信息交换反映了 OV 中三个基本体系结构数据元素——作战活动、作战节点和信息流之间的关系。

和信息交换相关的角色有信息功能提供者和信息使用者。与此相对应,OV-3 可以用两个单独的产品来描绘:① 提供的信息交换。它刻画并详述了与 NCE 可用的作战节点相关的信息;② 使用的信息交换。它刻画并详述了与需要从 NCE 中得到的作战节点相关的信息。

OV-3 是一个详细的表格,它详细描述了 OV-2 作战节点、OV-5 作战活动和 OV-6 相关的信息,还包括其他关于来自外部提供者的信息交换或信息授权使用等方面的信息。

### 3.4 组织关系图(OV-4)

NCE 中 OV-4 描述了服务功能提供者和服务使用者和支持网络中心信息共享的相关作战角色。它提供了所有必需的、述协作本质以执行网络中心行动(Net-Centric Operation, NCO)的组织关系。同时它将促进对外部、内部关系,用户类,作战概图及相关作战角色之间关系的理解。OV-4 层次描述还应该确保能够在全局信息栅格(GIG)的基础上开发能力和进行信息共享。

OV-4 可以用 UML 类图来表示,包括作战节点典型类和 UML 关系(如双向、无向、聚合、分解或泛化等),也可以通过用例图赋予参与者关系。

### 3.5 作战活动模型(OV-5)

NCE 中的 OV-5 描述能力、活动(任务)和按网络中心方式运行的节点间的信息流,从而力求并尽快发布信息和数据,以鼓励信息的新发现和重用。

由于 NCE 的核心理念是信息和能力来自于并贡献于网络化环境,因此网络中心 OV-5 将系统内活动与系统外活动之间的输入输出(I/O)流置于非常重要的位置,它同时强调使外部活动能够利用其信息的内部活动和导致从外部活动中使用信息的内部活动。

OV-5 可通过 UML 图或 IDEF0 图进行表示。

其中 UML 图包括用例图、活动图和时序图。它们反映了 OV-5 的不同方面。

### 3.6 作战规则模型、状态转移描述和事件跟踪描述 (OV-6a, 6b, 6c)

以上各个 OV 产品是对体系结构元素的静态结构及其关系进行建模,但只有这些元素的动态行为被建模从而融入体系结构的次序和时间特征时,许多关键特性才能被发现。OV-6 产品正是用来为体系结构的动态建模技术提供支持,它由三部分组成。

OV-6a 为作战规则模型,它指明了影响 NCE 中运行的体系结构的约束和作战政策,包括适用于提供的或使用的信息以及 NCE 中的能力的规则和政策。规则应该体现 OV-1 中的作战概念。在 NCE 中,当传递信息或使用能力时,提供者和使用者应该进行交互,因此必须有约束来管理它们之间交换的信息和能力;同时,提供或使用信息所需的基础设施应该由提供者和使用者共享,则需要定义规则和政策以对需要的基础设施进行分配、供应、管理和维护。另外,定义信息安全约束和政策以保证信息和能力基于登录控制、授权和认证从而传送到授权用户也是非常必要的。OV-6a 用文本表示。

OV-6b 为状态转移描述,它用来描述 NCE 中的服务(信息和能力)提供者与使用者之间的状态转移,这种转移是因 NCE 中的服务提供者 and 使用者向 NCE 发布信息或从 NCE 取得信息而产生的响应。OV-6b 获取状态、事件及提供者 and 使用者从 NCE 中使用信息和能力的行动。OV-6b 还应确定何时信息资源处于初始有用状态,何处信息可用并已发布到 NCE。它通常用 UML 状态图表示。

OV-6c 即事件跟踪描述,它表示了相关作战节点间发生的信息和能力交换的时间顺序,这些交换是在 NCE 中执行的活动的输入和输出。顺序强调了何时、多么频繁地发布给 NCE 或从外部来源得到信息和数据。OV-6c 确保每个作战节点,特别是具有服务功能提供者或服务使用者作战角色的作战节点,在执行 NCO 时能够在正确的时间得到所需的信息。OV-6c 可以用 IDEF3 模型或 UML 活动图表示。

### 3.7 逻辑数据模型 (OV-7)

网络中心 OV-7 定义体系结构域内的数据类型

(或实体)及系统数据类型间的关系。需要说明的是它着重:① 描述正在节点间交换的信息的数据类型;② 使用标准或通用性的利益群体 (Community of Interests, COIs) 指南确定领域词汇表、分类法和上层本体。网络中心性依赖于对通用理解的词汇和意义的使用,从而支持 NCE 中更好的信息共享。网络中心 OV-7 通过定义合作的 COI 一致同意的数据和数据间关系支持 NCE 中的数据可理解性。

OV-7 与规定数据元素和规则以促成各体系结构间一致数据表示的 CADM<sup>[4][6]</sup>是不同的。尽管都称为数据模型,OV-7 只是一个体系结构产品,描述的是特定体系结构域的信息。而 CADM 并不是体系结构产品,而是对 DoDAF 产品和体系结构数据的知识库的数据库设计。基于 CADM 的库可以存储体系结构产品,包括 OV-7 在内。

## 4 对我军C<sup>4</sup>ISR建设的启示

C<sup>4</sup>ISR 体系结构的视图——OV, SV, TV 和 AV 相互联系并共同反映了体系结构。NCE 中 C<sup>4</sup>ISR 体系结构视图产品描述为 C<sup>4</sup>ISR 系统的需求开发、结构设计和修改、系统集成提供了通用的、易于理解的表示方式。它通过描述组织如何:① 从 NCE 中使用信息和能力;② 在预先规定的用户内使信息和能力得到充分使用实际上也为开发支持网络中心能力的体系结构提供了方法和指导方针。

作战视图体现的是军事人员的视角,作战视图产品则是从军事人员角度对 C<sup>4</sup>ISR 体系结构框架的描述,它对 C<sup>4</sup>ISR 系统的需求开发和高层设计至关重要,而需求开发和高层设计又处于系统开发的早期阶段,失之毫厘则差之千里。鉴于此,我军应该高度重视建立体系结构描述框架,建议在充分论证的基础上,成立专门的组织机构负责实施,健全制度,着力开发支持互操作、互联互通和网络中心能力的视图产品描述框架和标准,以指导我军信息化建设实践;另外,应该加大对 C<sup>4</sup>ISR 体系结构研究的投入力度,加强研究的统一规划,争取集中力量办大事;最后,应及时跟踪国外体系结构方面的研究动向,借鉴外军经验,从而使我军的信息化建设走上一条又好又快发展的路子。

需要说明的是网络中心能力的实现是分步完成的,如图 1 所示。因此开发支持网络中心能力的

C<sup>4</sup>ISR 系统也应该按此等级分为若干步骤。

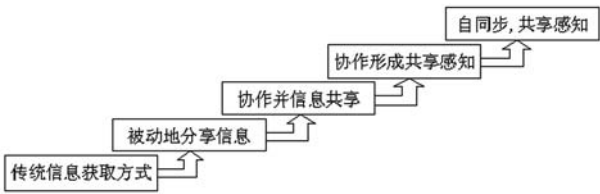


图 1 网络中心能力的实现步骤<sup>[5]</sup>

5 小结

本文对 NCE 中 C<sup>4</sup>ISR 体系结构作战视图产品进行了描述，它为开发支持网络中心能力的实际系统提供了指南，对我军的信息化建设具有很好的借鉴和指导作用。当然，目前我军的信息化水平与美军有较大差距，但如果我们立足信息化建设实际，充分吸收美军在 C<sup>4</sup>ISR 系统开发中的先进方法，则必将对对我军信息化建设的跨越式发展产生积极的促进作用。

参考文献

[1] DoD Architecture Framework Working Group. DOD Architecture Framework Version 1.0, Washington: DoD. 2003

[2] C4ISR Architecture Working Group (AWG) . C4ISR Architecture Framework Version 1.0, Washington: DoD, 1996

[3] C4ISR Architecture Working Group (AWG) . C4ISR Architecture Framework Version 2.0, Washington: DoD, 1997

[4] DoD Architecture Framework Working Group. DoD Architecture Framework Version 1.5, Washington: DoD. 2007

[5] David S. Alberts. Network Centric Warfare: Developing and Leveraging Information Superiority (2<sup>nd</sup> Edition) . Washington: CCRP Publication. 2000

[6] C4 Information Integration and Interoperability Directorate. C<sup>4</sup>ISR Core Architecture Data Model v 2.0. Washington: Office of the Assistant Secretary of Defense. 1998

作者联系方式

通信地址：西安第二炮兵工程学院基础部  
邮政编码：710025  
联系电话：15902902007    029-93348011



# 关于加强军事物流系统信息化建设的几点思考

葛林 傅历光 黄金虎

**摘 要：**军事物流系统信息化建设是我军信息化建设的一个关键环节，关系到我军现代军事后勤保障能力的提升。未来的信息化战争，后勤保障的重点将从依赖数量转向依赖速度和信息。如何充分运用信息化、数字化技术，在准确的时间、准确的地点为前方投送适量的资源成为现代军事后勤保障首要研究的重点，时间、空间、品种、数量及力量使用上的精确度已成为后勤保障保障高效的标志。为此，如何适应新军事变革挑战，积极创新发展，加强军事物流系统信息化建设，为打赢信息化战争提供坚实的保障能力，已经成为我们亟待解决的重要课题之一。

**关键词：**军事物流系统；信息化建设

“兵马未动，粮草先行”，这是古人用于描述后勤保障在军事作战行动中的重要地位和作用。随着二十一世纪新军事变革的不断深入发展，信息化战场将把后勤保障纳入到一个巨大的、与信息化武器相匹配的信息化作战体系中。通过“信息流”使保障力量集约化、社会化、远程化、智能化，作战力量战斗到哪里，后勤就确保保障到哪里，这将是未来信息化战争对现代军事后勤保障的要求。

军事物流信息化是现代军事后勤信息化保障的一个重要组成部分。以海湾战争为例，在 42 天的战争期间，多国部队耗资达 600 亿美元，平均每天耗资约 14.3 亿美元。整个战争，美军武器装备、弹药、油料和各种物资的消耗，单兵平均每日 200 余公斤，是二战时的 10 倍，越战时的 4 倍。如此庞大的物资消耗，以及品种繁多的物资种类，没有一个科学高效的军事物流信息化系统，是难以完成保障任务的。

## 1 军事物流及其发展概况

所谓的军事物流，是指采用信息化技术，将军事力量在平时和战时生活、训练、执勤及作战所需的军事物资，经过筹措、运输、包装、加工或生产、仓储、供应等环节，最终送达部队而被消耗使用，实现其空间（或与支配权同时）转移的全过程。军事物流的研究内容如图 1 所示，它主要对军事物流的基本理论问题、保障机制、技术平台构建、军事物资筹措与管理、军事物流中心构建、军事物资的储备和调度以及军事物资的运输与配送等

问题进行研究。

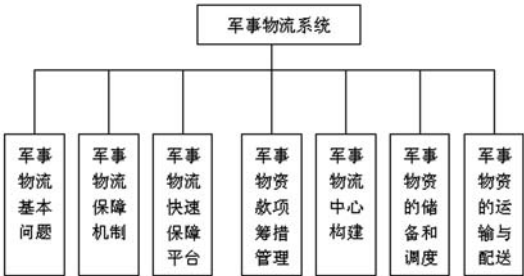


图 1 军事物流系统研究内容

从物流业发展的历史不难看出，美军在军事后勤运输领域的实践直接促成了军事物流概念的提出和发展。第二次世界大战期间，由于军队机动性能的提高和机动作战的需要，如何做好流动性部队的后勤保障工作，合理有效地实现军用物资调配，做到省时、省力、保障及时，成为军事后勤的一个突出问题。为此，美军利用运筹学方法展开研究，成功地解决了军事物资供应的诸多棘手问题，并形成了较为完整的军事物流理论。

经过几十年的不断发展，现代军事物流信息化建设相较之以往有了很大的发展。美军在军事物流技术的开发与应用方面走在了前列。美军在发展现代军事物流的过程中，广泛采取了搭建信息平台的方式，运用计算机信息网络链接物流运作的各个环节，对物流配送实体网络和信息网络进行“无缝链接”。20 世纪 90 年代初，美军就开始了“物流网点”的建设。由一个部门将过去几个部门分散管理的运输、补给、维修和其他保障职能统管起来。这个部门可以使用战场指挥通信渠道，了解作战部队的情况，掌握必要的指挥信息，因而能够准确预

测,甚至预先在战场上配置所需物资。

我军对军事物流信息化建设研究相比其他国家起步较晚。1984年,我军历史上第一个仓库教研室成立,该机构主要对军事仓库及军用物资储存进行理论研究及实践,这也是我军较早研究现代军事物流的机构。2001年,我军第一个军事物流仓储教研室正式成立。2003年5月16日,我军第一个军事物流工程实验室成立了。这标志着我军军事物流信息化建设跨上了一个台阶。但与其他国家相比,我军的军事物流信息化建设仍然存在着起步较晚、理论研究有待完善等不足。

## 2 军事物流系统特点

军事物流系统是一般物流系统的一个特例。除了具有一般物流系统的六个基本要素即流体、载体、流向、流量、流程和流速外,军事物流系统还具有特有的要素“时间”。军事物流的突发性特点,即军事物流需求发生的时间具有极大的不确定性和受时间约束的紧迫性,决定了在应急物流系统中“时间”是一个重要的系统要素。因此,军事物流系统具备有七个要素:流体、载体、流向、流量、流程、流速和时间。

与普通物流系统相比,军事物流系统具有如下不同的特点。

### (1) 军事物流系统的快速反应能力

军事物流系统最明显的特征就是突然性和不可预知性。军事物流系统的时效性要求非常高,要求必须在最短的时间内,以最快的流程和最安全的方式来进行军事物流保障。通常使用的物流运行机制已经不能满足应急情况下的物流需要,必须要有一套应急的物流机制来组织和实现物流活动。

军事物流的突发性和随机性,决定了军事物流系统应具有快速反应能力,具有一次性和临时性的特点。这一特点决定了军事物流系统区别于一般的企业内部物流或供应链物流系统的经常性、稳定性和循环性。

### (2) 军事物流系统的开放性和可扩展性

该特点源于突发事件的不确定性。由于人们无法准确地估计军事事件的持续时间、强度大小、影响范围等各种因素,从而使得军事物流的内容随之变得具有不确定性。

军事物流需求的随机性和不确定性决定了在军

事物流系统的设计上,应具有开放性和可扩展性。军事物流需求和供给在突发前是不确定的,必须在突发之后将其纳入军事物流系统中。

### (3) 时间效率重于经济效益

军事物流最大的一个特点就是“急”字,如果运用普通物流理念,按部就班地进行将无法满足不同紧急的物流需求。在一些重大的突发事件中,经济效益原则将不再作为一个中心目标加以考虑。因此军事物流目标具有明显的弱经济性,甚至在某些情况下成为一种纯消费性的行为。

军事物流的突发性、流量不均衡性和时间约束的紧迫性决定了在军事物流中时间效率重于经济效益。军事物流的流向、流量及其精确性、预见性如何,不仅起着支持和保障军事行动的作用,还发挥着调整 and 强化军事后勤力量,将国家的经济力、科技力转化为战斗力,以及支援和巩固国防建设的作用。

## 3 多法并举,加强军事物流系统信息化建设

军事物流信息化是军队信息化建设的一个重要组成部分,也是有中国特色军事变革的需要。推进我军信息化建设,其中关键环节就是要多法并举,加强有我军特色的军事物流系统信息化建设。

### 3.1 统一领导,走一体化发展道路

军事物流系统信息化建设涉及面广,牵涉到军事准备的方方面面。必须加强统一领导,统一规划,搞好顶层设计,按照统一的规划思想、标准规范和技术体制,走一体化发展的道路,确保我军军事物流系统信息化建设健康有序地向前发展。

走一体化发展的道路,一是要加强集中统一领导,强化管理落实。军事物流系统作为现代军事后勤保障的关键环节,必然要求建立一整套完善的高度集中的联合机制。必须以总部相应领导机构为基点,以各战区为节点,建立一套行之有效的军事物流信息化联合指挥机制,加强对军事物流信息化的统一领导。在加强集中统一领导的同时应分工明确,落实责任。二是要统一规划,搞好系统集成。军事物流信息化涉及部门众多,涵括了指挥、控制、通信、后勤、装备等众多部门。必须深入研究分析,在明确军事需求和系统结构的基础上,按

照统一的规划、统一的技术标准、统一的技术体制,搞好顶层设计。要强化综合集成,实现各级各类系统的连通,从而实现我军军事物流系统的综合一体化,在联合作战中最大限度地发挥整体效能。

### 3.2 统筹兼顾,加强军地物流一体化建设

物流战场是沿整个国家物流设施网络形成的作战空间,具有明显的军民兼容特征。物流战场建设对军队战略部署、国防要素配置都有直接而深远的影响,事关国家长远安全利益,美军军事物流系统就呈现出军地物流一体化的趋势。1999年,美陆军器材部根据“批发级后勤现代化计划”,通过合同方式,将“产品司令部标准系统”和“标准仓库系统”外包,由民间企业负责其运行与维护工作。加强我军军事物流系统信息化建设,同样应遵循军事物流发展规律,走军地物流一体化建设道路。

加强军队物流一体化建设,必须将军事物流纳入国家物流建设总体规划之中,同步建设,并行发展,做到一次建设,军地互益;必须通过国家的社会经济发展计划,把军事物流设施建设同地方物流基础设施建设结合起来,铁路、公路、机场、码头等大型物流基本建设应严格贯彻军事要求,地方大型物流系统设计建设应“军地一体,民为军用”;必须研究制定军事物流平战转换、民军转换的理论、机制,充分利用民用物流,为军事物流的实施提供强有力的支撑和保障。

### 3.3 综合集成,加强军事物流信息化平台建设

加强军事物流信息化建设,一方面要求提升军事运输装备技术水平,另一方面也要求重视先进物流技术在军事物流领域的应用,加强军事物流信息化平台的建设。

加强军事物流信息化平台建设,一是要注重基础设施,加强信息传输平台综合集成建设。信息传输平台是信息化军队的神经网络,也是军事物流信息化建设的基础。没有信息传输平台作为基石,军事物流系统信息化建设将无从谈起。为此,要加强

计算机通信网络等基础性信息传输平台的建设。二是要注重高新技术的应用。军事物流的效率在很大程度上取决于新兴信息技术的应用程度,必须加强综合集成条码技术、射频识别技术(RF)、电子数据交换(EDI)、全球定位系统、地理信息系统、卫星通讯技术等高新技术。三是要注重对关键技术的研究与实现。军事物流系统涉及到大量关键技术,如军事物资保障方案的优化选择、军事服务设施点优化选址、军事物资调度、路径优化选择和军事物资装载等等。应加强对这些关键技术的理论研究和实现,并将这些智能技术最大限度地融入到军事物流系统平台中,从而更好地为军事后勤保障提高辅助决策依据。

### 3.4 人才为本,加强军事物流系统信息化人才队伍建设

军事物流系统信息化对科学技术发展具有很高的敏感性,对高素质信息化人才队伍的需求也较高。没有高素质的信息化,很难建设出一个科学合理高效的军事物流系统,效能也难得以充分发挥。目前我军军事物流系统人才普遍知识面单一、专业不对口,缺乏既懂军事信息化技术又懂军事物流、军事后勤保障的高素质人才。为加强我军军事物流系统信息化建设,必须坚持人才为本,建设培养一支高素质的军事物流信息化人才队伍。

人才为本,建设培养一支高素质的军事物流信息化人才队伍,一是要统筹规划、制定人才培养规划。必须立足我军军事物流系统发展现状,着眼于未来发展,统筹规划,优先制定人才培养规划,并加以落实;二是要多渠道培养,完善培训机制。可采取军队院校与部队人才双向交流、军队与地方共同培育人才、积极同外军交流等方式多渠道培养高素质军事物流信息化人才;三是要创造留人环境,充分发挥人才作用。应创造良好条件,建立竞争机制,最大限度地发挥各类人才地主观能动性,从而做到人尽其才,才尽其用,充分发挥出高素质人才的科研攻坚、学术带头、传帮带和组织领导等作用。

参考文献(略)

作者联系方式

通信地址:福建省军区自动化站

邮政编码:710068

联系电话:0591-24950041

# 美军卫星通信现状、发展趋势及对我军卫星通信发展的启示

郭道省 张邦宁 刘爱军

**摘要：**首先，阐述了美军卫星通信的现状，并对其技术体制进行归纳；然后，分析、总结了美军卫星通信的发展趋势；最后，根据我军卫星通信目前的发展状况，为我军卫星通信下一步发展提出几点设想或建议。

**关键词：**美军卫星通信；技术体制；发展趋势；我军卫星通信发展的设想

## 1 概述

信息技术的迅猛发展以及在军事领域的广泛应用，使作战思想、军队体制编制以及战争形态发生着革命性的变化。突出表现为：① 远程精确打击武器装备上非常有效的传感器和指挥控制系统，将成为未来战争的主导因素；② 信息战，先进的信息技术大大地增强了军事信息系统实时收集、处理、传递与利用信息的能力，可以对军事行动实施有效的支援。与此同时，保护己方信息系统的有效性和连续作战能力，并能削弱、摧毁或破坏对手信息系统的作用，将成为作战中优先考虑的问题。

鉴于空间独特的地位和在未来信息化战争中的重要作用，空间优势将成为 21 世纪军事战略的重要组成部分。以卫星为主体的航天信息系统将是一体化全球信息感知、全球指挥控制系统的核心，全球卫星导航定位系统将成为未来中远程精确打击和精确兵力投送的关键装备。因此，航天信息系统也成为各国竞相发展的技术制高点。1998 年 4 月，美航天司令部公布了具有战略意义的军事航天长远规划——2020 年设想。该规划指出，空间力量将成为 21 世纪美国实施国家安全与军事战略的主要依靠力量，美国空间力量的首要任务是夺取空间优势。

作为航天信息系统的重要组成部分——卫星通信，其在现代战争中发挥着越来越大的作用。美军对卫星通信的依赖性日益增强，在阿富汗战争中，卫星通信承担了 78% 以上的战区通信任务，在海湾战争中，90% 以上的情报靠通信卫星传送，在伊拉克战争中，美军不仅使用军用卫星，也几乎用尽了商用卫星的可用资源。

与地基的其他通信系统相比，卫星通信具有其

独特的优势和作用：

- 能够大范围全球覆盖，也可以区域覆盖甚至点覆盖；
- 具有点对点，一点对多点及广播的通信功能；
- 根据需要，可以实现网络的覆盖、连接、容量及业务负载的再组合或者再分配；
- 可以大、中、小及微型地球站并存，且能够在陆地、海上和空中使用；
- 网络建立时间短，开通快。

本文将重点阐述美军卫星通信的现状、技术体制和发展趋势，最后根据我军卫星通信的发展状况，对我军卫星通信下一步发展提出几点设想。

## 2 美军卫星通信系统的现状和发展趋势

### 2.1 美军现有卫星通信系统的现状

美国的军用卫星通信系统包括战略通信卫星系统、战术通信卫星系统和战略战术通信卫星系统。战略通信卫星提供全球的战略指挥、控制、通信和情报传输，其中包括各种侦察卫星获取的信息和数据的传输，战略通信卫星的代表是国防卫星通信系统（DSCS）。战术通信卫星则提供地区性战术通信，包括军用飞机、舰船、车辆，乃至小分队或单兵背负终端的移动通信，战术通信卫星的代表是舰队通信卫星系统（FLTSAT）、空军卫星通信系统（AFSAT）和特高频后续卫星（UFO）通信系统。战略战术卫星通信系统是军事星（MILSTAR）卫星通信系统。MILSTAR 是美海、陆、空各军种的一项联合任务计划，是美国为确保冷战时期核战争

条件下的三军保密通信，于 80 年代初开始实施的一项军事卫星通信系统工程，是美国战略系统中绝对位居首位的计划，也是美国政府实现战略/战术

部队现代化的一个关键卫星通信系统。图 1 是美军卫星通信在数字化战场上的使用示意图。

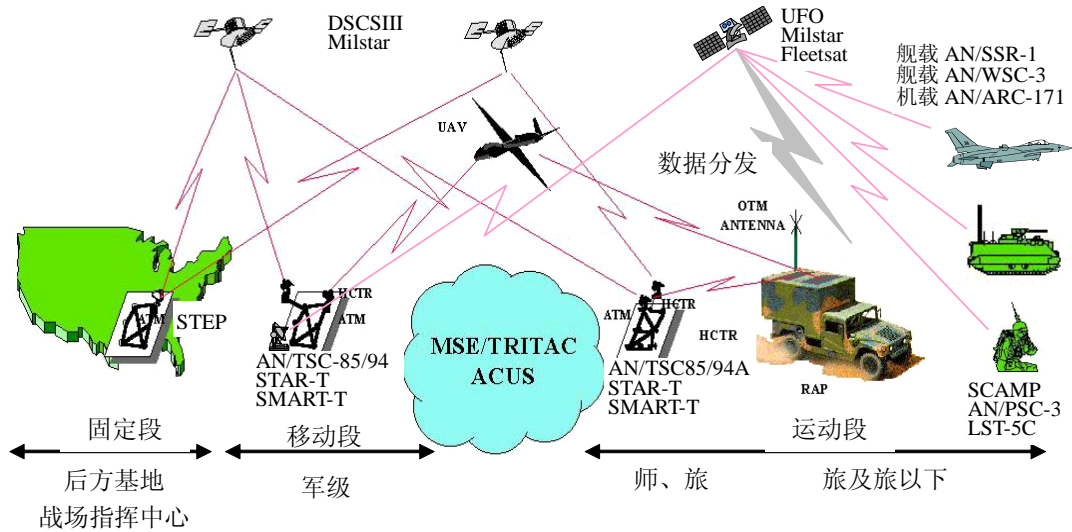


图 1 美军卫星通信在数字化战场使用示意图

按照频段划分，美军卫星通信系统涵盖了 UHF、SHF 和 EHF 频段，其中 UHF 频段的代表系统是特高频后继星（UFO），SHF 频段的代表系统

是国防卫星通信系统（DSCS），EHF 频段的代表系统是军事星（Milstar）系统，如表 1 所示。

表 1 给出了美国军事卫星系统的主要工作频段及其代表系统

	主要频段	可用带宽	代表系统	频段特点
UHF	225~400MHz	500KHz	FLTSAT UFO	技术成熟，移动站不需跟踪
SHF	C (4/6GHz)	36MHz	INTELSAT 等民用系统	通信容量大，巨大的商业资源
	X (7/8GHz)	50~80MHz	DSCS	主要的干线通信频段
	Ku (11/14GHz)	72MHz	INTELSAT 等民用系统	通信容量大，巨大的商业资源
EHF	Ka (20/30GHz)	1~1.5GHz	UFO/GBS	容量大，降雨损耗大
	20/44GHz	1/2GHz	Milstar	容量大，抗干扰能力强

下面分别介绍这几种卫星通信系统中典型系统的特点和信号体制。

2.1.1 UFO（特高频后继星）

“特高频后继星”（UFO），它是替换“舰队卫星通信系统”的新一代窄带卫星通信系统，具有容量大、功率高的特点，且与“舰队卫星通信系统”使用的终端兼容。第 4 颗 UFO 卫星是 UFO 系列中第 1 颗带有极高频通信有效载荷，且抗干扰、遥测、控制、广播和舰队间通信能力有所加强的卫星，其极高频有效载荷使卫星信道数增加了 11 个。另外，在 1998—1999 年发射的第 8、9、10 颗 UFO 卫星上还搭载了采用 Ka 波段的“全球广播

系统”（GBS）转发器，使通信实力大增。使用 UHF 频的空军卫星通信系统和舰队卫星通信系统可向作战飞机、海面船只和水下舰艇提供窄带保密通信和全球广播通信。其发展趋势是采用最新的数字化技术，利用软件无线电概念，发展新型的 UHF 终端，使其不仅能够接入卫星通信系统，而且还能够和地面无线系统互通。

其使用频段为 225 ~ 400MHz，带宽为 500KHz。该系统有各类通信终端：如舰载站、潜艇站、机载站、陆上车载站和背负站等站型。可以传送的业务包括：FM 模拟话、24kb/s PSK 调制的声码话、75b/s FSK 电传与 1.2~9.6kb/s PSK 数据。部分信道采用了按需分配的时分多址方式，可

在一条 25kHz 带宽的信道中容纳 13 条 1.2kb/s 数据或 7 条 2.4kb/s 保密话, 经过按需分配可供数百用户使用。系统中大量应用了跳频调制解调器。

归纳起来, 其信号传输体制为: 窄带系统, 对不同的业务, 速率为 75b/s、24kb/s、1.2~9.6kb/s 等几种。调制方式为 FM、PSK、FSK, 多址方式为 FDMA、TDMA 和跳频。多址分配方式为预分配和按需分配的结合。

### 2.1.2 DSCS (国防卫星通信系统)

最新的国防卫星通信系统为第三代国防卫星通信系统 (DSCS-3) 它用于为美军各军兵种提供全球通信, 即在重要军事终端与国家指挥机关之间提供话音、数据、数字和电视传输, 主要是为大容量固定用户提供保密的话音和高速数据率通信。其标准星座由 5 颗工作星和至少 3 颗备用星组成, 采用超高频, 具有抗核打击和抗干扰能力。

该系统的终端几乎都采用了跳频/直接序列扩频技术, 并且可多载波工作。地面机动部队使用终端为扩频调制解调系统, 扩频带宽为 20MHz, 可提供传输速率为 75b/s~4999kb/s 的数据或话音。空军的机载终端同样为直接序列扩频终端, 可处理 75b/s 电传、2.4kb/s 声码话和多路数据。海军部门使用的终端可提供话音和数据, 速率为 16/32kb/s。情报部门使用的终端可提供数据和话音, 其速率可在 75b/s~1.544Mb/s 变化, 皆有抗干扰措施。

归纳起来, 该系统的技术体制为: 业务为话音和数据, 速率从低速到高速可变, 采用跳频/直接序列扩频技术, 可多载波方式工作, 其他抗干扰措施还包括可控多波束天线。

### 2.1.3 Milstar (军事星)

1994 年 3 月, 首颗 MILSTAR (DFS-1) 卫星发射入轨, 1995 年 11 月, 第二颗 MILSTAR (DFS-2) 卫星顺利升空, 两星配对工作, 提供对美军太平洋至大西洋部队的抗干扰保密通信覆盖, 业务以低速数据 (LDR) 为主。第二代 MILSTAR-2 (DFS-3, 4, 5, 6) 卫星在 2002 年前全部发射升空, 从而形成全球覆盖的抗干扰卫星通信网, 能提供中速数据业务 (MDR)。美军目前正在研制容量更大、性能更好的 MILSTAR-3 卫星——“先进 EHF”计划。

Milstar 的技术特点包括:

- 采用 EHF 频段: 上行 44GHz (EHF), 带

宽为 2GHz, 下行 20GHz (SHF), 带宽为 1GHz。支持 UHF/SHF 和 EHF/UHF 交叉频带通信业务, 以便于 DSCS 及 FLTSAT 系统兼容。

- 采用宽频带扩频: 上行线路采用 FDMA, 在 2GHz 带宽上的全频段快速跳频; 下行线路采用 TDMA 和加快速跳频, 跳频速率每秒近万次。
- 采用可控点波束天线和快扫描多波束自适应调零天线技术, 它在感受到敌方干扰后, 能通过幅相控制迅速将天线方向图的零点指向敌方干扰机。
- 具有星上处理、交换功能: 采用星上信号处理技术; 具有广泛的星上信号处理能力, 卫星成为一个空间交换中心, 可自动控制与各系统的连接、自动控制到终端用户的传输路径, 这可减少对复杂地面设备的依赖, 并能大大简化地球终端。
- 星间链路: 卫星之间使用 60GHz 的直通线路, 在地面设施受核破坏下可用此线路迂回, 及减少远距离通信时对两跳中继的依赖, 而且由于 60GHz 通过大气层时基本上被吸收, 有效地减少地面侦听其星际链路的可能性。
- 采用先进的纠错技术, 具有强纠错能力。
- 能用较小尺寸的天线阵获得高方向性的传输, 增加了敌方截收信号的困难, 另外 EHF 可以有效对抗核辐射。
- 具有低速率 LDR 和中速数据率 MDR 信道, 低速为 75~2400b/s, 中速为 4.8kb/s~1.544Mb/s。

Milstar 系统的具有三级控制功能, 包括: ①系统控制, 实施卫星运行控制监测、空间资源分配, 由美国本土的空军基地来完成; ②战术控制, 对所分配资源进行动态规划、监视, 具有网络自适应能力, 由各战场指挥中心完成; ③星上自主控制, 卫星的位置与姿态的调整在长达半年的时间可不需地面的支持。

归纳起来, 该系统的技术体制为: 业务为话音和数据, 速率从低速到中速可变, 采用 EHF 频段, 采用宽带快速跳频技术, 上行为 FDMA/FH, 下行为 TDMA/FH, 具有星上处理、星上交换和星际链路能力, 采用可控点波束天线技术和天线调零



技术等多项抗干扰技术措施, 整个卫星系统具有三级控制。

## 2.2 美军卫星通信系统的发展趋势

考虑到现有系统的性能下降将无法满足未来战场和天基系统对信息传输的需求, 结合其转型计划, 美军大力增强现有系统的通信能力, 大力发展新型卫星通信系统。对于这些新系统, 要求其具有支持全球信息栅格 (GIG) 和网络中心战的能力。

这些新系统的具有以下显著特点:

- 更大容量、更宽带宽、更高数据率和吞吐量;
- 大容量激光通信;
- “动中通”;
- 先进的天线技术;
- 面向基层战斗部队、分队服务。

这些新系统主要包括:

- 窄带 - MUOS (移动用户目标系统);
- 宽带 - WGS (wideband gap satellite, 宽带添隙卫星) 和 AWS (Advanced Wideband System, 先进宽带系统);
- 抗干扰 - AEHF (先进极高频系统)、TSAT (APS) (转型卫星、先进极地卫星)。

纵观这些新系统的特点, 可以看出, 美军卫星通信系统具有以下几个方面的发展趋势。

### 2.2.1 从UFO到MUOS: 全面提升全球UHF战术卫星通信系统的窄带通信能力

UHF 频段由受气候和遮蔽等自然环境影响较小, 非常适合于战术移动通信场合, 从 Fleetsat、UFO 一直到目前规划的 MUOS 系统, 美军仍在大力发展 UHF 频段战术通信系统, 用以向数目众多、成本低廉、携带方便的战术终端提供窄带通信。特别是移动平台对 UHF 终端的需求非常大, 目前 UFO 系统估计有 7500 个终端。

移动用户目标系统 (MUOS) 是替代美“特高频后继星” (UFO) 系统的美国海军下一代移动卫星通信系统。MUOS 是一个窄带卫星通信系统, 可为世界范围内、多军种/多国的移动和固定战斗终端提供通信服务。MUOS 从体制上进行众多的改进, 以 CAI 空中接口替代早期的 DAMA 系统, 使用了 Turbo 编码的新型可变速率调制编码技术, 大大提高在恶劣条件下系统的可用度, 使系统的可用

度 90% 提高到 99%。新型 MUOS 系统采用具多波束天线的星上处理有效载荷, 并利用星际链路能力, 大大提高网络可靠性。

MUOS 通过 DAMA 方式支持以前的 UHF 终端, 新的 UHF 手持式终端使用新的公共无线接口 (CAI), 允许高效可靠的网络控制, 新的控制信道使用的 20/30 GHz 频率, 不同卫星系统之间可通过 DISA 的 Teleport 进行。以前的 UHF 终端可通过 MUOS、DISN 和国防部拥有的网关与商用 MSS 系统互通, 新型终端可直接实现与 MSS 终端的互通, 新型手持式终端遵循联合战术无线电系统体系 (JTRS), 能与应急无线电系统和联合战术无线电系统互操作。

### 2.2.2 宽带卫星通信系统: 从DSCS到WGS和AWS, 容量进一步提高

宽带填隙卫星 (WGS) 系统是一种高容量军用卫星通信系统, 完成 DSCSIII 服务寿命增强计划 (SLEP)、全球广播系统 (GBS)、有效载荷以及弥补减轻 DSCSIII 万一失效时的冲击影响, 它们一起提供从现在到 AWS 建成这一过度时期的宽带服务。与目前的国防卫星通信系统 (DSCS) 和全球广播服务 (GBS) 系统相比, WGS 可以为用户提供更新、更快的卫星通信业务和超高频宽带通信业务, 并将成为 DSCS 与未来的 AWS 系统之间的联系桥梁。在 WGS 上采用 10 个 Ka 频段可控波束, 采用相控阵技术的 8 个 X 频段波束和 1 个全球覆盖 X 频段喇叭天线。通信容量从 DSCS III 的 100Mbps 和 DSCS SLEP 的 200Mbps 提高到 3.6Gbps。

先进宽带系统 (AWS) 是为满足国防和情报界对宽带需求以及中继通信系统的需求而设计的。该系统将使用激光通信技术, 并作为 DSCS、GBS 和 WGS 的后续系统。AWS 卫星将容量提高到 10Gbps 以上。利用 GBS 卫星向战场分发数据, 进一步增强战场态势感知能力。AWS 计划已和五角大楼的以激光为基础的“转型卫星通信系统” (Transformational Satcom System - TSAT) 合并, TSAT 最终将替代美国国防部现有的卫星系统, 并作为先进极高频 (AEHF) 卫星系统的补充。

该系统采用星地激光传输, 星座的吞吐量约 10~40Gb/s。作为全球信息栅格 (GIG) 的天基系统组成部分, TSAT 将 GIG 延伸到没有地面连接的用户, 提供更好的连接性及数据传送能力, 极大地

改进战斗员使用的卫星通信。转型卫星通信系统的目的是作为支持 NASA、DoD、IC 等机构的各个天基系统的独立但可互操作的分系统的一部分，提供改进的、有生存力的、抗干扰的、全球覆盖的、安全的、而且是通用的通信服务。TSAT 支持的整个 GIG 的实现意味着战斗空间的每个资源都是可寻址、可接入，可用来产生、处理、传输信息。

这些系统主要采用的技术有：

- 点波束和相控阵天线；
- 星上处理、再生和星上微波交换技术；
- 大功率卫星平台（15-35KW）；
- 电子推进系统；
- 激光通信技术。

### 2.2.3 从MILSTAR I、II到ACTS：进一步增强抗干扰通信能力

在 MILSTAR I 卫星的基础上，在 MILSTAR II 上增加了中速率有限载荷，最高链路的速率达到 1.544Mbps，满足了中继链路抗干扰能力需求。2003 年 1 月，美国军方委托 L-3 通信公司建立美国新一代军用通信卫星网络 ACTS。该系统采用星上处理技术、星际链路技术以及轻型多功能通信天线的组合阵列和宽带频率合成技术等。并在 MILSTAR II 的基础上进一步增强抗干扰通信能力，将单信道抗干扰链路的速率提高到 8Mbps，整星容量为 MILSTAR II 的 10 倍。即使发生灾难事件，该系统也可以提供可生存的、全球的安全通信。其星座包括 4 颗可相互交叉通信的卫星，它们覆盖南北纬 65° 间的广大地区，每颗星有 50 多个信道，传输速率可达 500Mbps。卫星从 2006 年开始发射，2008 年全部进入轨道，最终取代“军事星”（MILSTAR）系统。

主要采用的技术有：

- 点波束天线和调零天线；
- 多波束跳变技术；
- 星地一体化宽带跳频技术（上行 2GHz，下行 1GHz）；
- 星上处理和星上交换技术；
- 星上网控、路由、加密及自主控制技术；
- 与 UHF 交链技术；
- 星际链路。

### 2.2.4 采用更加先进的天线技术

天线技术的特点主要体现在以下几个方面：

- 多点波束天线的规模达到 200 以上；
- 大型可展开天线的口径最高达到 150 米（电子侦察用）；
- 天线所使用材料更新、重量更清、工艺更先进；
- 大型可展开天线技术（12 米以上）和有源相控阵多波束天线技术（200~300 个点波束）；
- 数字波束形成技术和光学波束形成技术；
- 多频段大型可展开反射器天线及其动态高精度跟踪；
- 同时跟踪多个飞行器（20 个）技术；
- 多波束干扰自适应调零和可控定向点波束天线。

### 2.2.5 其他先进技术

这些新技术包括：

- 星上处理技术：现今多数通信卫星还是用透明弯管式转发器，在未来的新一代卫星，尤其是军用通信卫星中，星上再生、解扩、解跳、交换等的应用，将使卫星成为有抗干扰能力的空中网络控制及信息处理中心，适应复杂的电磁环境和通信流量变化，有效地利用信道资源，保障通信。
- 扩展频段和多频段共用：从 C、Ku 向 Ka 及 EHF 频段扩展，激光通信。
- 星间链路（毫米波、光）。
- 高功率和功率按需分配（SSPA、TWTA 和矩阵功放）。
- 动态链路分配（DLA）技术。
- 星载高性能微处理器和存储器。
- 星地、星星信息融合技术。
- 微波信道的小型化、固态化技术。

## 3 对当前我军卫星通信发展的启示

通过对美军军事卫星通信的现状描述和发展趋势分析，对比我军军事卫星通信的现状，我们还有较大的差距。为了在将来高技术信息化战争条件下“打得赢”，我们要立足国情，积极进取，大力发展我军新一代具有较强战场生存能力和抗干扰能力的军事卫星通信系统。

借鉴美军卫星通信系统和体制的特点和优势，



可为我军卫星通信下一步的发展提供以下启示。

1) 研究先进的天线技术, 包括星上大型可展开天线技术、多波束天线技术和调零技术, 并研究结合先进天线技术的星上处理模式和信号传输体制。

2) 必须要大力发展高频器件, 特别是超高频、极高频技术器件, 摆脱核心器件依靠进口的根本问题。

3) 星上处理和交换技术, 包括可变速率星上处理技术、星上动态链路分配技术、多波束系统中网络管理与控制技术, 多波束系统下的子网划分、资源分配、安全管理、波束切换技术等。

4) 星上网络控制、管理技术和加密技术。

5) 抗干扰技术, 包括新型的抗干扰技术体制、对付多种干扰样式以及复杂的干扰模式的新型

参考文献 (略)

#### 作者联系方式

通信地址: 解放军理工大学通信工程学院卫星通信教研室

邮政编码: 210007

联系电话: 025-80828050

抗干扰技术措施, 提高中高速业务的抗干扰通信能力和最低限度通信能力。

6) 研究新型的编码调制技术, 提高系统容量、降低终端尺寸。

7) 卫星通信网与其他网系的融合技术。

## 4 结束语

本文着重阐述和分析了美军卫星通信系统的现状和发展趋势, 并结合我军卫星通信系统的现状和研究成果, 基于进一步扩大系统容量和覆盖范围、进一步提高系统组网灵活性和抗干扰能力, 对我军新一代卫星通信的发展提出一些设想或建议。

# 对构建海军天基信息应用体制的思考

黄 晷 杨根源 牛利勇

**摘 要：**从海军作战实践需求与天基信息装备现状的主要矛盾入手，分析了海军作战对天基信息应用体制的需求，给出了建立海军天基信息应用体制的基本原则，在此基础上通过研究提出了海军天基信息应用体制组织体系结构和海军天基信息应用机构的建立方案。

**关键词：**海军作战；天基信息；应用体制

海军天基信息应用体制是关于海军将天基信息装备和天基信息资源应用于支援海军作战的组织体系、机构设置、职能划分、相互关系及法规制度的统称。目前，海军所特有的天基信息装备种类、数量都很少，大部分的天基信息装备是由总部管理和控制<sup>[1]</sup>。因此，建立适应海军作战实践需求的天基信息应用体制，在制度上保障海军对天基信息装备和天基信息资源有序、顺畅的运用，对于海军在未来联合作战中充分发挥作战效能，更好地履行总部赋予海军的新世纪新阶段使命任务具有十分重要的现实意义。

## 1 海军作战对天基信息应用体制的需求分析

### 1.1 海军作战实践需求与天基信息装备现状之间的主要矛盾

第一，海军作战对天基信息的需求量大，而我军天基信息装备数量有限。海军作战空间广阔、战场环境复杂、兵力分散、协同难度大，对战场信息的依赖程度特别高。天基信息装备在信息获取与传输上与海军现有的信息装备相比具有作用距离更远、覆盖范围更广、时效性更强的特点，因此，海军作战特别需要来自天基信息装备的信息支援。然而，目前我军天基信息装备种类和数量有限，难以满足在未来联合作战中海军单独组织诸兵种合同作战和海军参加诸军种联合作战背景下的海洋侦察监视、信息传输保障、导航定位和海洋环境监测的需求。

第二，海军作战对天基信息的时效性要求高，而申请天基信息支援的过程复杂。信息化条件下的

战场态势瞬息万变，海军作战对天基信息的时效性相应地提出了很高的要求。目前我军的天基信息装备主要是由总部直接管理和控制，海军诸兵种作战力量若需天基信息装备进行信息支援，就必须向海军、总部逐层提出申请，经审批后由总部统一接收所需的天基信息资源并加以处理，再向海军分发，最后由海军转发到诸兵种作战力量。从海军诸兵种作战力量提出申请到将天基信息应用于作战这整个过程需要通过层层申请与审批，其时间延迟可达数小时甚至数天之多，难以满足海军作战对天基信息的高时效要求。

第三，海军作战对天基信息的准确度要求高，而现有天基信息装备能力不足。面对信息化条件下日渐复杂的海战场环境，加之现代战争中战场伪装欺骗与干扰手段的多样化，海军作战对天基信息装备获取的卫星侦察信息、导航定位信息和海洋水文气象信息的准确度要求也越来越高，而我军天基信息装备的建设正处于起步阶段，各种天基信息装备的作战能力尚不完善，很难有效地保障天基信息的准确度。

### 1.2 构建海军天基信息应用体制是解决矛盾的最有效途径

通过分析海军作战实践需求与天基信息装备作战应用现状的矛盾不难看出，解决这些矛盾最简单的方法就是增加我军天基信息装备的数量，提高天基信息装备的作战能力。但是增加和研制作战能力更强的天基信息装备要由总部进行科学论证与长远规划，一方面需要耗费大量的人力和物力，另一方面也需要花费大量的时间，短期内难以有效解决问题，这种做法是与我军“坚持把科学发展观作为加强国防和军队建设的重要方针”这一指导思想相背

离的。当前,应该遵循科学发展观的思路和要求,立足现有的天基信息装备,建立适应海军作战实践需求的天基信息装备作战应用体制,合理、高效、科学地利用天基信息资源才是解决矛盾的最有效途径。

建立海军天基信息应用体制,有利于合理地调整海军诸兵种作战力量对天基信息支援的需求,对总部分配给海军的天基信息装备和天基信息资源进行统筹管理和科学分配,大大提高有限的天基信息装备的利用率;建立海军天基信息应用体制,能够缩短申请天基信息支援的中间过程,避免因层层申请和审批而降低天基信息的时效性,从而高效地利用天基信息资源;建立海军天基信息应用体制,可以对现有的天基信息装备和天基信息资源进行科学组合和综合处理,有效地提高天基信息的准确度。

## 2 确立海军天基信息应用体制的原则

海军天基信息应用体制的确立应以服从海军作战实践需求为总的原则,与我军天基信息装备能力现状相适应,做到集中统一、机构合理、法规健全,保证天基信息装备能够顺畅、高效地应用于支援海军作战。

### 2.1 集中统一

集中统一是确立海军天基信息应用体制的根本依据,其实质是权力的集中和指挥的统一。首先,要明确我军天基信息装备的管理与控制权在总部,海军天基信息应用机构只对分配给海军的天基信息资源具有高度集中的管理权限;其次,确立海军天基信息应用体制时必须对所属的各级应用部门赋予明确的职责权限,理顺各部门相互间的关系;第三,海军天基信息应用体制作为海军作战指挥体制的重要组成部分,它的作战应用活动应与海军诸兵种作战行动紧密结合,受海军最高作战指挥机构的统一指挥和领导。

### 2.2 机构合理

天基信息应用机构是海军天基信息应用体制的“硬件部分”,它的建立应从海军作战实践需求出

发,结合我军天基信息装备的能力现状,科学地设置天基信息应用机构内部各级应用部门并编配相应的人员,合理地区分各级应用部门及相应人员的职能、权限。同时,要在保证天基信息资源快速、及时地应用到支援海军作战的前提下,尽量减少天基信息应用机构内部的纵向层次和横向跨度,从而使整个天基信息应用机构达到高效运转。

### 2.3 法规健全

法规是用以规范海军天基信息应用机构内各级应用部门和相应人员实施作战应用活动的行为准则,是确立海军天基信息应用体制的基本保证,也是海军天基信息应用体制中不可或缺的“软件部分”,对于保障天基信息装备的作战应用活动顺畅进行有着十分重要的作用。只有在健全、严密的法规约束下,天基信息应用机构内各级应用部门和相应人员才能更好地发挥主观能动性,保证整个作战应用体制的顺利运行,从而有力地支援海军作战。

## 3 海军天基信息应用体制组织体系构想

海军天基信息应用体制组织体系是海军借以实现天基信息装备作战应用职能的、相对稳定和完整的应用系统组织形式,在很大程度上受到海军现行的编制体制的影响和制约<sup>[2]</sup>。根据海军在未来联合作战中可能的参战形式,遵循上述海军天基信息应用体制的确立原则,可将海军天基信息应用体制组织体系结构分为海军单独组织诸兵种合同作战背景下的作战应用体系和海军参加诸军种联合作战背景下的组织体系两种模式。前者的基本结构为:海军合同作战司令部——天基信息应用中心——下属各作战应用中心的三级组织体系,如图1所示。后者的基本结构为:战区联合作战司令部下属海军作战指挥机构——天基信息应用中心——下属各作战应用中心,如图2所示。

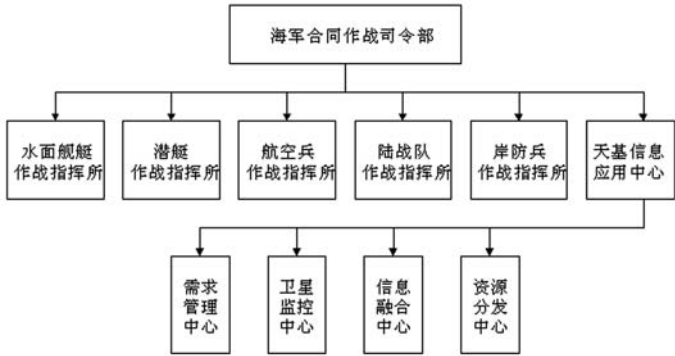


图 1 海军单独组织诸兵种合同作战背景下天基信息应用体制组织体系结构

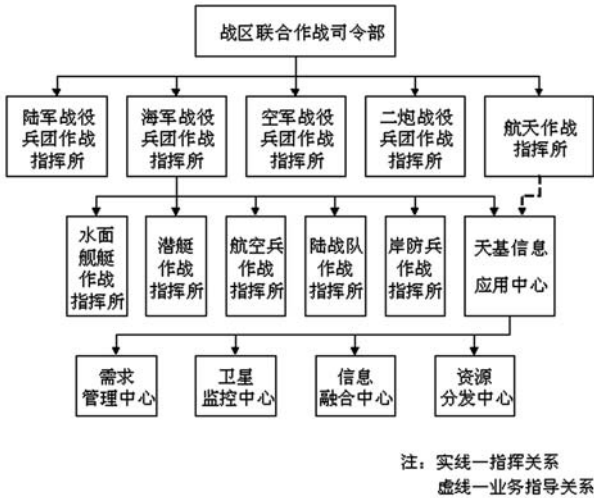


图 2 海军参加诸军种联合作战背景下天基信息应用体制组织体系结构

4 海军天基信息应用机构建立方案

海军天基信息应用机构是海军天基信息应用体制的重要组成部分，是对总部分配给海军的天基信息装备和天基信息资源实施控制和管理的核心机构，它的建立是天基信息装备高效、顺畅地应用于支援海军作战的重要保证。考虑海军作战实践需求以及目前天基信息装备的能力水平和作战应用现状，可在海军天基信息应用中心下设立需求管理、装备监控、信息处理和资源分理四个相互支持、相互配合的作战应用中心。

需求管理中心主要由海军司令部的作战部门人员并吸收部分诸兵种的作战部门人员组成，其主要职责是根据海军作战任务需求向总部提出天基信息装备和天基信息资源申请；接收来自诸兵种的天基信息需求申请，对所提需求进行统筹、协调，形成初步的天基信息资源分配方案，并提供给资源分理中心；拟制天基信息装备作战应用计划，提供给天基信息装备监控中心。

装备监控中心是以从总部抽调负责天基信息装备管理与控制的有关人员为主，再加上部分必要的作战、情报部门人员组成，其主要职责是与遍布全国的卫星测控站联网，不间断地监视总部分配给海军的天基信息装备的工作状况；按照天基信息装备作战应用计划，控制、督导总部分配给海军的天基信息装备实施各种作战支援活动。

信息处理中心主要由从总部情报部门抽调的参谋、技术人员和海军司令部情报部门的参谋、技术人员组成，其主要职责是接收各类侦察卫星和环境监测卫星发来的天基侦察信息和天基环境监测信息；运用各种战术或技术手段对所接收的各类天基信息迅速进行判读和综合处理，形成可直接利用的情报信息，并提供给资源分理中心。

资源分理中心是由海军司令部的通信参谋人员并吸收部分诸兵种的通信参谋人员组成，其主要职责是依照需求管理中心确定的天基信息资源分配方案，统一分配和分发通信卫星的频段资源和经信息处理中心处理后的情报信息资源；对有价值的情报

信息进行分类和存储,建立侦察信息和环境监测信息数据库,并与诸兵种相关数据库保持经常性的更新。

## 5 结束语

研究和构建海军天基信息应用体制是海军在新的历史时期履行肩负的使命任务和应对面临的威胁

挑战的客观要求,不仅符合以科学发展观为指导的海军建设发展的重要方向,而且将成为提升海军战斗力的一个新的、强有力的增长点。当前,应抓住我军跨越式发展的有利时机,建立并完善海军天基信息应用体制,为从根本上提升未来信息化战争中海军作战能力奠定良好基础。

## 参考文献

- [1] 孟涛. 海军航天信息作战问题研究. 北京: 信息对抗学术, 2005.1, 24~26
- [2] 杨根源. 战役信息作战指挥问题研究. 北京: 国防大学出版社, 2001.5
- [3] 母仕民等. 关于确立军事航天指挥体制的探讨与思考. 装备指挥技术学院学报, 14/4, 2003.8, 47~51
- [4] 冯书兴等. 空间作战指挥体制问题研究. 装备指挥技术学院学报, 15/1, 2004.2, 51~54
- [5] 常显奇等. 军事航天学. 北京: 国防工业出版社, 2005.1

## 作者联系方式

通信地址: 海军航空工程学院指挥系

邮政编码: 264001

联系电话: 13884931412

# 美俄军队信息化建设基本策略刍议

姜明远 于滨

**摘 要：**美俄军队信息化建设的基本策略，涉及其为保障军队信息化发展建设指导思想、基本原则、目标和重点等军队信息化发展战略的实现而采取的一系列政策性的方式、方法，以及直接为军队信息化建设从现实状态向期望状态过渡而采取的具体措施等。美俄军队的信息化建设起步较早，经过了较长时期的发展建设，积累了许多经验和教训，具有一定的代表性。加强美俄军队信息化建设基本策略问题研究，对于促进军队信息化建设具有一定的借鉴意义。

**关键词：**美军；俄军；军队信息化；发展建设；基本策略

上个世纪末期以来爆发的高技术局部战争的实践，各国充分认识到信息技术广泛渗透到军队建设的各个领域可使军队的战斗力发生质的飞跃。因此，加快军队信息化建设步伐已成为各国共同的选择。美国、俄罗斯等军事强国的装备信息化建设走在了世界前列，提出了许多新观点，积累了较多成功经验，值得研究、借鉴。

## 1 美军信息化建设基本策略

自从 20 世纪 80 年代以来，美军就开始有组织、有计划地展开了军队信息化的建设。经过近三十年的不懈努力，美军的军队信息化建设已走在了世界的前列，初步构建起了信息化武器装备体系。其成功经验、做法对其他国家的装备建设有着巨大的示范和启迪效应。

### 1.1 理论先导

美军认为，建设信息化军队是一项极其艰巨而复杂的军事系统工程，需要提出相应的理论和文件进行通盘筹划和指导，而且必须经过长期不懈的努力才能完成。因此，在经过 20 世纪 90 年代前半期以信息化建设为核心内容的“军事革命”理论探索之后，美参联会于 1996 年 7 月出台了《2010 年联合构想》；美国防部于 1997 年 5 月公布了《四年防务审查报告》。这两份文件是美军全面推行军队信息化建设的第一代纲领性文件。2000 年 5 月和 2001 年 9 月美军又分别推出了以《2020 年联合构想》、《四年防务审查报告》为代表的第二代纲领性

文件。根据上述两代文件规定的总体框架，各军种又相继制定了适合本军种特点和要求的信息化发展策略，如陆军的《2010 年陆军构想》和《后天的陆军》；海军的《后天的海军——对未来技术的构想》和《2010 年海军构想：前沿……由海向陆》；空军的《全球作战——21 世纪空军构想》和《全球参与——21 世纪空军构想》等。这种总目标和分目标相互结合的方法，自上而下地将美军装备发展规划纳入一个完整的体系，使其装备信息化建设得以有计划、有步骤地进行。

### 1.2 虚拟实践

在传统的军队建设过程中，世界各国通常遵循“有什么武器打什么仗”的思维模式。由于无法预测未来战争中出现的新情况和新特点，使得军队的建设发展很难满足战争的需要。信息化时代，由于“虚拟现实”技术的飞速发展，使得预测战争发展趋势，有针对性地发展武器装备，即“打什么仗发展什么武器”成为可能。美军已提出，今后在其装备建设中将根据未来战争的需要，运用“虚拟现实”、“系统仿真”等技术手段，创造一种模拟未来战争的“人工合成环境”，如未来战场、未来训练场等，让军人在这种虚拟环境中进行“预实践”。通过这种“预实践”的实验、检验、完善、论证，得出有关数据和结论，用以指导发展未来作战理论、制定作战预案、设计武器装备，进而调整军队指挥体制与部队编制，规划武器装备的发展，改进院校教育和部队训练。为了采用“虚拟实践”的方法加强军队建设，特别是加强军队信息化建设，美国建立了许多“战斗实验室”、“作战模拟试验室”或

“作战仿真试验中心”，以便在其创造的虚拟环境中，利用虚拟现实系统，经济有效地进行军事训练、作战模拟和新式武器装备的研制开发，科学合理地确定科技发展重要领域。

### 1.3 统一标准

美军在信息化建设初期，各军兵种共有指挥信息系统一百多个。这些彼此“烟囱式”林立的系统增加了战场信息相互融合的难度，带来了信息流程的离散化，很难实行跨层次、跨军兵种进行联合作战的信息获取、传递与处理，而且采购、使用、维护和改进费用都很高，经济上难以承受。为了确保未来作战系统间保持可靠的互联、互通甚至互操作性，自 1991 年以来，在国防部副部长直接组织领导下，美军先后制定和发布了一系列有关体系结构的指导性标准文件，如《信息技术基础设施体系》、《信息技术标准指南》、《技术参考模型》、《信息管理体系结构框架》、《联合技术体系结构》、《C<sup>4</sup>ISR 体系结构框架》、《国防信息技术设施通用操作环境》等，确定了技术标准、法规和惯例，为整个军事信息系统的体系结构开发、表述和建立，规定了协调一致的途径与框架，并从总体上定义了实现联合作战各作战要素之间的互联、互通甚至互操作所应具备的各项能力，通过制定作战体系结构、技术体系结构和系统体系结构等视图结构，来实现军事信息系统的一体化建设和互联互通互操作性能。

### 1.4 措施配套

为了创造良好的军队信息化发展环境，美军根据军队信息化的要求，进行了大刀阔斧的改革。如重新设计国防部的职能程序，提高效率；将商业领域的技术管理方法用于军队建设，以经济承受能力为核心，加速武器装备的信息化建设。美国各军兵种也采取了一系列改革措施，如美国海军成立了海军需求监督委员会。该机构由海军作战部常务副部长负责管理，负责确认海军的需求，并向联合需求监督委员会提供代表海军立场的报告。美国国防部还制定了旨在保护关键基础设施和确保信息安全的各类措施，如发展一体化探测和预警敌方攻击的能力；改进信息收集系统和反情报手段，大力发展卫星、无人机及人工情报系统，并通过保密、隐蔽等手段降低敌人的情报探测能力；为了提高有关人员的积极性，美军还准备增设信息军官配套措施，以

促进军队信息化建设发展。

## 1.5 军民结合

美军在军队信息化建设过程中，极大地得益于其规模庞大、实力雄厚的民用商业信息技术市场。美军认为直接采用民用商业技术不仅节省了装备研究和开发资金，而且将其用在重要的军事领域中，能更容易地获得和保持信息化武器装备所需的互联、互通和互操作性能。因此，美军认为必须继续促进和加强对通用商业标准的利用，必须继续利用商业信息技术，直接购买和租用民用商业现有信息技术和设备，以提供未来所需的强有力的“即插即用”式基础设施。与此同时，美国还涌现出了一大批积极主张进行新军事变革、实施军队信息化建设的地方军事理论家。例如，“国防预算研究中心”主任克雷派尼维奇、战略与国际问题研究中心政治军事研究部副主任古雷、兰德公司高级研究员比伊尔德、著名未来学家托夫勒夫妇等。他们认真研究军事变革的历史沿革，军事变革发生的动因、内涵和影响，以及美国应当采取的具体措施等军队信息化建设发展的重大问题，为美国进行军事改革和军队信息化建设进言献策，提供了有益的舆论准备和理论支持。

## 2 俄军信息化建设基本策略

为了适应未来军事斗争的需要，防止北约东扩、维护国家安全战略环境，俄军高度重视军队信息化建设。在规划军队发展时，始终把提高军队的整体信息化作战能力放在十分重要的位置，形成了适合本国国情的军队信息化建设道路。

### 2.1 政策指导

俄罗斯为了推进其军队信息化建设，分阶段出台了有针对性的指导性政策文件。1993 年之后，俄罗斯相继提出了《俄罗斯联邦军事学说基本原则》、《2005 年前国家武器装备发展计划》。2000 年初，普京就任总统后，先后签署了《俄罗斯联邦国家安全构想》、《俄罗斯联邦军事学说》，并于 2000 年 9 月，批准了《俄罗斯联邦信息安全学说》。此后，普京还签署了《信息战理论》等政策文件。这一系列的指导性政策文件，逐步明确了俄罗斯军队

关于信息化建设的主要观点：一是赢得侦察、监视、目标截获系统以及智能指挥与控制系统等信息化武器装备的优势，将在克敌制胜中起决定性作用；二是提高信息化作战能力是提高军队作战能力的最有效手段，武器系统要力求信息化、智能化；三是重点保证 C<sup>4</sup>ISR 与电子系统发展；四是将信息作战优势作为衡量未来军队质量建设的重要指标。这些指导性政策文件的出台，为今后一段时期内俄罗斯军队信息化建设指明了方向。

## 2.2 理论牵引

俄军认为，要取得未来信息化战争的胜利，军事理论研究工作一定要先行。因此，俄军十分重视对军事革命、军事信息技术、信息武器和信息战等方面理论的深入研究，提出了一系列非常有影响的军事理论和学说。20 世纪 90 年代以来，俄罗斯军事理论发生了重大变化：一是基本的作战思想从大纵深作战理论发展为大纵深立体作战理论；二是基本作战样式由方面军群战役发展为战区战略性战役；三是传统的快速集群发展为战役机动集群。俄军提出的“作战系统理论”，强调在统一的指挥控制下，立体战场的整体协调配合，形成综合一体的作战系统。同时，作战行动强调打击敌作战系统的关节点，以较少的军事投入取得较大的军事效益。在此基础之上，俄军认为“未来战争必将是使用以精确制导武器为主的高技术战争，高精度武器已成为现代战争的主要突击力量”，因此十分注重远距离作战行动，即利用各种精确制导武器在尽可能远的距离上先敌实施火力打击；强调电磁与火力相结合的突击行动，即在压制和摧毁敌方电子器材和信息系统的前提下，加强火力突击的效果，使电子战起到与火力突击效果相辅相成的作用；强调与敌信息战武器之间的积极对抗行动，确保军队在信息化战争条件下的生存力和战斗力。

## 2.3 技术带动

俄罗斯的经济实力今非昔比，目前尚不能展开军队信息化的全面建设，只能有选择、有重点地发展关键的技术领域，改进急需的武器装备，以求能够较快地带动全军装备信息化建设的步伐。因此，俄军十分重视对重点军事新技术尤其是军事信息技术的发展预测，强调要运用最新科技成果、最新工艺、最新材料来超前研制新一代武器装备，制定了

“俄军武器装备发展长期规划”，决定优先发展精确制导武器、空军装备及机动部队、运输工具，并进一步提高战略武器的威力以及机动性、可靠性。重点加强微电子和计算机技术、雷达技术、电子对抗技术以及人工智能等关键性技术领域的研究工作，大力发展高精度洲际弹道导弹、潜射弹道导弹和巡航导弹；发展作战效能不受大气层和天气因素影响的新一代精确制导机动弹头；发展隐身作战平台及其信息化武器弹药等；发展新型超视距雷达、可见光和红外线波段雷达等探测设备；发展定向能、电磁脉冲等新概念武器；发展全球监控、获取和处理信息的综合系统；研制军用机器人和智能武器。

## 2.4 信息主导

俄军认为，无论在战争时期还是在平时时期，信息战不仅可对敌方军事目标造成重大破坏，而且可对敌方国家政权和管理机关的基础设施构成严重威胁，已成为国家军事潜力和部队战斗力的重要增长点。信息战武器的使用同常规武器、核武器或化学武器不同，尚没有受到国际监督和条约的严格限制，这将对军事指挥控制网络较为发达的军事强国构成更大威胁。俄前国防部长谢尔盖耶夫称，信息战武器将替代目前的大规模杀伤性武器，是“本世纪最令人恐惧的武器”，“要把信息战武器作为国家军事政治和战略潜力的组成部分，列入长期军备发展计划和重要的科研课题”，“以赶超的速度开展科研和设计工作”。为此，俄军加强了信息战的研究，并提出了一系列战法。例如：实施主动信息攻击措施，对敌计算机网络实施破坏，阻塞网络中的信息流动等。在作战理论的牵引之下，俄军已开始研制信息战“早期预防系统”，并加强了无线电电子对抗设备、声音合成器、超高频震荡器、信息病毒及其“埋置”、大气信息图像等信息战武器的研究项目，军用侦察卫星、无人侦察机、干扰机、自导辐射武器运载器的研制项目已取得了明显进展。

## 2.5 注重太空

高技术局部战争的实践让俄军更加清楚地认识到，太空将成为未来高技术信息化战争的主要作战空间，建立和保持以太空优势为主的全维优势是未来战争致胜的一个重要法宝。空间、空中、地面已成为不可分割的一个整体，要赢得未来战争的胜



利，就必须加强包括外层空间在内的全维攻防能力。因此，俄军提出了研制“往返式航天系统”的发展构想。该系统可实施战略与战术空间侦察，也可实施太空战，以高精度武器打击敌地面目标。此外，俄军还将为新组建的“天军”装备新型反卫星武器，用于攻击敌方部署在地球低轨道上的预警探测、情报侦察、通信、导航定位、气象等卫星以及

航天飞机等空间信息化武器设施；对现有的一百余颗军用和民用卫星进行新技术改造；研制和发射新型的地球大气及海洋观测卫星和各种军用侦察卫星、空间侦察系统，以及最先进的导航定位卫星等；为“天军”装备最新式的侦察和打击型卫星及导弹，发展太空监视与防御系统、国家及战区导弹防御系统，增强其早期预警能力。

### 参考文献

- [1] 朱小莉. 美俄新军事革命. 北京: 军事科学出版社, 1996.10
- [2] 费肖竣. 美国军队信息化建设研究. 北京: 国防大学出版社, 2003.6
- [3] 李辉光. 美军信息作战与信息化建设. 北京: 军事科学出版社, 2004.8

### 作者联系方式

通信地址: 空军指挥学院 4235 信箱

邮政编码: 100097

联系电话: 13683312795    010-66925756

# 建立军事信息系统灾难备份与恢复体系相关问题思考

李军让 高岩 宋焱淼

**摘 要:** 信息系统灾难备份与恢复越来越凸现其重要性。本文首先对灾难备份恢复技术及其规划方法进行探讨, 然后针对军队当前信息系统建设现状, 提出了建立军事信息系统灾难备份与恢复体系规划中应注意的几个问题, 最后对灾难备份恢复技术未来研究方向进行简要分析。

**关键词:** 灾难恢复 (Disaster Recovery); 灾难备份; 生存性 (Survivability)

## 1 引言

随着我军信息化建设的逐步深入, 信息系统在指挥控制、情报、训练、管理等方面发挥了越来越重要的作用, 各项军事工作越来越依赖于军事信息系统。而病毒、黑客、误操作、软硬件故障、自然灾害、敌方攻击等各种客观原因, 都可能导致各种程度的军事信息系统灾难, 对信息系统及数据安全造成了极大威胁<sup>[1, 5]</sup>。基于高速网络的数据备份与灾难恢复技术能充分保护军事信息系统中的重要信息, 保证灾难发生后信息系统的持续运行, 在计算机和信息安全领域已经成为一个研究热点。

美国的“911”事件以及事件后世贸中心信息系统的快速恢复用事实说明了灾难事件的现实性, 以及灾难恢复规划的必要性<sup>[10]</sup>。因此, 针对我军目前信息系统开发应用现状, 依托国防通信网和地下防护措施, 规划建设我军军事信息系统远程容灾备份体系已经变得非常迫切。

## 2 信息系统灾难备份恢复技术

### 2.1 灾难备份恢复的必要性

信息系统的灾难并不限于传统意义上比如像洪水、飓风和地震等自然灾害, 还包括一切造成正常业务流程非计划中断的所有事件, 如电力故障、通信基础设施中断、敌方攻击、犯罪破坏活动以及由病毒、黑客攻击、硬件损坏、误操作等引起的大规模系统故障<sup>[2, 3]</sup>。

灾难恢复是在灾难发生时确保信息系统保持连续运行的过程。这个过程不仅是主要功能和系统的

恢复, 而且强调所用时间尽可能短。灾难恢复规划就是为了减少灾难事件的可能性以及限制灾难对关键业务流程所造成的影响而制定灾难恢复计划的过程及一整套行为。执行灾难恢复计划的目的在于不管引起灾难的原因是什么, 都要快速、有效和经济地恢复系统运行<sup>[3]</sup>。由于灾难事件的无法控制、预测及其引发后果的严重性, 灾难恢复规划就变得非常重要。

### 2.2 灾难备份恢复目标

灾难备份和灾难恢复是降低灾难发生的损失、保证计算机系统连续运行的重要措施, 是信息系统安全的最后一道屏障。灾难备份是指为了减少灾难发生的概率, 以及减少灾难发生时或发生后造成的损失而采取的各种防范措施, 它的主要目标是保护数据和系统的完整性, 使业务数据损失最少甚至没有业务数据损失。灾难恢复是指计算机系统灾难发生后, 在远离灾难现场的地方重新组织系统运行和恢复运营的过程<sup>[2]</sup>, 它的主要目标是业务快速恢复, 使业务停顿时间最短甚至不中断业务。

为了有效的对灾难恢复目标进行衡量, 工业上常用的指标有两个: 恢复点目标 RPO (Recovery Point Object) 和恢复时间目标 RTO (Recovery Time Object)。RPO 指灾难发生后数据必须能够恢复到某一时刻的要求, 也就是灾难发生时刻与最近一次数据备份时刻的最大可容忍时间间隔。RPO 时间越小, 数据的丢失越少, 所以对于数据依赖性比较强的业务应该给予较小的 RPO 值; RTO 指系统从灾难发生到重新恢复运行的时间, RTO 越小, 系统的恢复能力越强, 所以对于要求具有较高连续性的业务系统应该给予较小的 RTO 值<sup>[4]</sup>。

## 2.3 灾难备份与恢复技术

信息系统的灾难备份与恢复技术通常包括数据存储备份、数据远程复制等数据容灾技术以及基于多节点负载均衡及集群的应用容灾技术。容灾系统的设计阶段为了满足恢复时间目标 RTO 和恢复点目标 RPO, 必须评估各种不同的技术。每种技术具有不同的 RTO/RPO 特点, 各有其优点, 也有其不足的地方<sup>[9]</sup>。一个完整的、有效的容灾方案, 必须包括多种技术手段的组合才能完成。下面分别对这两类容灾技术进行简要说明。

数据备份是把数据复制到备份介质上, 通常采用离线方式保存数据, 它的 RPO 为上一次一致性备份的时间, 它的 RTO 为从备份介质中恢复的时间 (包括: 运送磁带的的时间, 系统配置时间, 数据恢复时间), 典型情况下需要 1~3 天时间或更长。

数据复制根据复制模式可分为同步复制、异步复制、周期性的复制; 根据复制技术的不同可分为磁盘卷镜像、硬件复制、数据库复制和基于主机的复制 (逻辑卷或文件系统)、应用复制。同步复制模式要求数据只有在同时提交给主节点和备份节点后, 才能确认数据, 并进行后续操作。同步复制模式能保证数据的 RPO 在秒级, 但同步模式通常会对系统的性能产生较大的影响, 对网络带宽要求较高, 整体投资较大, 运营成本较高, 支持的距离有限。异步复制模式不要求数据在主备节点同时提交, 数据首先在主节点提交, 然后系统可处理后续服务, 然后才在备份节点提交。异步数据复制模式典型的 RPO 在分钟的级别, 异步数据复制对带宽要求较低, 支持的距离通常不受限制, 但会造成一定的数据丢失, 同时也有数据被毁坏的危險性。周期性的数据复制模式, 定期建立与主节点的数据同步, 典型的 RPO 在小时的级别, 对带宽要求较低, 但要求系统有充足的存储余量<sup>[8]</sup>。

在数据容灾的基础上, 可以构架应用容灾。典型的应用容灾机制包括: 多节点负载均衡和集群技术。负载均衡适合于非交易应用, 典型的应用如 Web 服务、应用服务器。对于交易类型的应用, 通常采用集群技术来提供恢复机制, 集群技术能自动检测失效并切换到备用节点。

## 3 信息系统灾难恢复规划方法

信息系统灾难恢复规划项目和通常的大型系统开发项目一样复杂, 它贯穿于整个系统开发生命周期, 其各个阶段及其相互间关系如图 1 所示<sup>[2]</sup>。

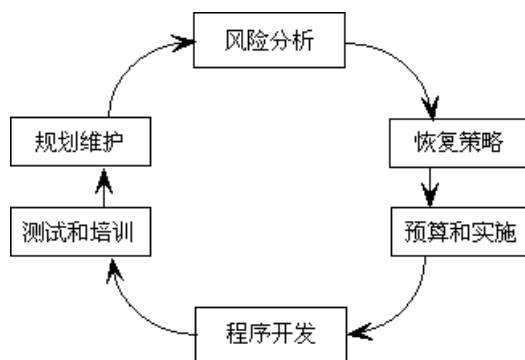


图1 灾难恢复规划项目周期图

1) 风险分析阶段: 鉴别信息系统中潜在的威胁和漏洞, 量化风险和各種中断损失, 识别关键应用, 定义恢复时间目标 RTO 和恢复点目标 RPO。

2) 恢复策略制定: 根据前一阶段的分析结果, 确定恢复策略和合适的技术体制, 定出任务的优先级。

3) 预算和实施: 明确规划开发所需要的花费, 并且制定出规划的时间和资金预算。部署用以支持恢复策略所需要的备份系统。

4) 程序开发: 联系供应商, 购买产品和服务, 开发恢复程序, 并且将程序文档化。

5) 测试和培训: 对系统进行测试和改进, 对人员进行培训。

6) 规划维护: 把测试得到的改进内容加入系统, 进行周期性的检查、修改和维护。

## 4 军事信息系统灾难恢复规划思考

军队作战指挥、控制、情报等信息系统对持续可用性和数据安全性提出了更高的要求, 这些系统的瘫痪将造成不可估量的损失, 因此针对军事信息系统的灾难恢复规划就显得更为重要和紧迫。我军在信息系统灾难恢复规划方面还处于试验及起步阶段, 缺乏整体考虑与对抗大规模灾难的准备, 与美军存在较大的差距<sup>[5]</sup>。在我军军事信息系统灾难恢复规划中应注意以下几个方面的问题。

#### 4.1 建立全军统一规划的灾难备份恢复体系

容灾系统的部署不但涉及到昂贵的大型磁盘阵列、光纤通道交换设备、磁带库及大型存储管理软件,还需要高带宽的通信链路资源,系统总成本极高。从目前的信息化现状来看,单一部门关键业务少,为其建立单独的容灾备份体系必然造成极大的资源浪费。另外容灾备份系统是一个全新的领域,系统的后期维护对人员有较高的要求,各部门独立的灾难备份体系容易造成维护成本的升高以及各个部门间维护质量的参差不齐。

为了提高容灾系统的利用率与数据共享效率,同时吸取我军指挥自动化系统建设中曾经烟囱林立的教训,建议采用统一的技术体制,以地域划分,建立地区性灾难备份中心,为本地区所有部门的关键业务提供灾难备份与恢复支持。选用成熟、统一、具有良好兼容性及可扩展性的技术体制,在全军建立多个灾难备份中心,各个灾难备份中心间互相形成异地容灾,大大提高数据的可用性、安全性。

#### 4.2 加强容灾备份体系中的数据安全性建设

军事数据的安全性具有至关重要的意义。保证应用系统及数据的机密性、完整性,防止非授权访问也是容灾系统建设中很重要的一个方面。

目前灾难备份恢复系统所用到的各种技术体制均存在不同方面的安全问题。存储区域网 SAN 在光纤通道数据帧认证和光纤通道交换机等方面都容易受到攻击,虽然国际上关于 SAN 安全性的研究已经取得了一些进展,但还有许多方面有待提升。NAS 的安全性、备份恢复数据流的安全性等问题也都要引起重视,可以通过引入认证机制或者在通信过程中使用加密技术对其安全性加以改进。

另外要实现灾难备份体系中生产中心与备份中心间数据的异地安全传输,就必须要在互连的线路上接入线路保密机,线路保密机要求能实现 FC 到 FC 的线路加密,以及高速链路的线路加密。而目前 FC 线路保密机国内和军内没有产品,必须加紧自行研制开发。

#### 4.3 重视系统建设的同时也要重视灾难恢复规划及演练测试

灾难备份恢复系统的建立只是说明信息系统具

备了灾难恢复的能力,在灾难发生后能否有条不紊地快速恢复系统的运行还要依赖于灾难恢复规划及灾难发生前的演练水平。要按照灾难恢复规划方法写出军事信息系统恢复策略和程序,并形成一系列文档。该系列文档应能对可能损害军事信息系统的任何灾难加以考虑,详细说明在灾难发生之前、之中和之后应当采取的行动。

该系列计划需要仔细推敲并得到相关负责部门认可,要对其进行预先测试,以保证灾难发生后能够快速有效地进行恢复。测试过程中对灾难恢复计划中所制定规程的有效性和适当性进行评估,以检查其完备性和实时性,发现并纠正缺点。

#### 4.4 加速自主知识产权容灾备份体系的研究与实现

目前,灾难恢复系统的研究和产品还主要集中在国外,如 IBM, EMC, Veritas 等国际知名的大公司都有自己的灾难恢复系统产品,其中融合了 SAN、NAS、远程镜像、RAID、集群等技术<sup>[11]</sup>,功能非常强大。依托这些成熟的商业产品来构筑军事灾难备份恢复平台,可以大大加快部署速度,提高军事信息系统的可用性安全性,但这些商业产品内核技术不公开,对我们来说完全是一个黑盒子,用其作为核心军事业务支撑系统存在安全隐患。另外,这些商业产品售价昂贵,系统建设及后期维护代价极高。

基于以上考虑,我军有必要分阶段有计划地加紧进行自主知识产权的容灾备份体系的研究。具体包括以下几个方面。

1) 对商用灾难备份恢复系统进行移植,使其支持我国或军队自行研制的安全操作系统。例如,在该操作系统上开发支持主流 HBA 卡的驱动,使这些专用操作系统平台能够接入光纤通道 SAN 存储网络。

2) 研究支持通用硬件平台的复制软件、数据备份软件与集群软件。解决基于通用硬件平台的远程数据同步/异步复制;开发支持专用数据库系统的并具有良好安全性能的数据备份软件;开发我军自己的集群软件,实现对目前已有军事应用的高可用支持。

3) 在此基础上,随着国内硬件研发能力的增强,可以进一步研制拥有完全自主知识产权的大型智能化磁盘阵列、磁带库等硬件。只有掌握了灾难

备份恢复系统软硬件的核心技术,研制出符合我军军事信息安全要求<sup>[8]</sup>的灾难备份恢复系统,才能真正保证军事信息系统的高安全性和可用性。

事应用系统的可用性及数据安全性,战时能保证在被打击情况下系统地及时恢复甚至不间断运行,具有非常重要的意义,因此需要加大规划、建设力度。另外国内外关于“可生存性技术”<sup>[7, 10]</sup>的研究也能提高系统在极端情况下的可用性,具有很好的研究与借鉴意义。

## 5 结束语

信息系统灾难备份与恢复平时能够提高核心军

## 参考文献

- [1] Nelson K. Examining Factors Associated with IT Disaster Preparedness[C]. System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference. Volume 8, 04-07 Jan. 2006 Page (s): 205b - 205b
- [2] J W Toigo. Disaster Recovery Planning, Preparing for the Unthinkable, Third Edition [M]. New York: Prentice Hall PTR, 2001
- [3] R J Sandhu. Disaster Recovery Planning[M]. Premier press, 2003
- [4] H Garcia-Molina, C A Polyzois. Issues in Disaster Recovery[A]. IEEE Compcon[C]. 1990. 573-577
- [5] Smith D R, Cybrowski W J, Zawislan F, Arnstein D et al. Contingency/disaster recovery planning for transmission systems of the Defense Information System Network[J]. Selected Areas in Communications, IEEE Journal on Volume 12, Issue 1, Jan. 1994 Page (s): 13 - 22
- [6] Hayes P E, Hammons A. Disaster recovery project management[C]. Petroleum and Chemical Industry Conference, 2000. Record of Conference Papers. Industry Applications Society 47th Annual 11-13 Sept. 2000 Page (s): 55 - 63
- [7] Hiles A. Surviving a computer disaster[J]. Engineering Management Journal. Volume 2, Issue 6, Dec. 1992 Page (s): 271 - 274
- [8] 王德军, 王丽娜. 容灾技术研究[J]. 计算机工程. Vol 31, No.6 2005.3
- [9] 张艳, 李舟军, 何德全. 灾难备份和恢复技术的现状与发展[J]. 计算机工程与科学. Vol 27, No.2 2005
- [10] 黄遵国, 卢锡城, 王怀民. 可生存技术及其实现框架研究[J]. 国防科技大学学报. Vol 24, No.5 2002
- [11] 刘颖娜, 李涛, 赵奎. 一种基于 Internet 的灾难恢复系统的设计和实现[J]. 计算机应用研究. 2005
- [12] 罗强一, 刘建涛, 宋自林. 军事信息系统集成的核心是数据集成[A]. 中国电子学会电子系统工程分会第十一届 C3I 系统与理论学术年会, 2004-11, 中国宁波[C]
- [13] GJB 2824-97, 军用数据安全要求[S]. 北京 1997-12

## 作者联系方式

通信地址: 北京市海淀区复兴路 20 号自动化站

邮政编码: 100840

联系电话: 010-66816465 010-66816468

# 对比外军发展谈我军信息资源的开发与利用

李连 李晓奎 邱立军

**摘要：**搞好军队信息化建设，并以信息化带动战斗力提高，是我军当前的一个重大战略决策。信息资源开发利用作为军队信息化的核心任务，也是当前我军工作的重中之重。加快标准体系建设，完善评估机制，提高自主创新水平都是搞好信息资源开发利用的有效途径。

**关键词：**信息化；信息资源开发；标准体系建设；体制创新

当前，以信息化建设为核心的新军事变革正在飞速向前发展，加快信息化建设，已成为各国军队的共同目标。面对新的国际形势，我军正在以科学发展观为指导，积极推进新时期的军队信息化建设，努力以信息化带动战斗力。为有效地实施这一方针，在大量调研工作的基础上，本文从我军信息资源开发利用的现状、需要注意的问题和未来发展趋势等三方面，对推进我军信息化建设进程的相关问题进行论述。

## 1 当前我军信息资源开发利用的现状

### 1.1 标准体系不健全，缺少成熟的信息资源共享和应用机制

继美军的战略 C4ISR 系统之后，印度也凭借自身在信息技术领域的优势，在新德里建成了全军信息处理中心，实现了联合参谋部与陆海空三军司令部之间的信息共享。然而，我军目前对信息资源开发利用还缺乏科学、系统的规划，没有从法规制度上去规范信息资源开发利用的方法、途径和标准等根本性问题。由于标准规范不统一，也缺乏对开发人员的统一组织和领导，大多数部门现有的数据资源开发体系和标准规范都不相同，不利于实现系统的互连互通和信息资源的交互共享，开发出大量孤立、分散的软件系统，制约了信息的集成和共享。

### 1.2 实用价值不明显，缺少完善的信息资源评估和验收机制

近年来，我军在信息资源开发利用上做了不少

工作，但仍然存在对信息资源开发利用重视程度不够的问题，导致所开发资源的利用率不高，严重制约了建设总体水平的发展和提高。具体表现在以下几个方面：一是针对性不高。一些系统在开发前，缺少详细的业务考察和需求分析，没有经过严格的评审就仓促上马，结果是还未推广，就遭淘汰，造成资源的严重浪费。二是推广力度不够。一些业务人员存在惰性心理，不愿意更改传统的工作方式，对新开发的系统积极性不高，不愿学，不愿用。三是适应性不强。许多系统对信息资源开发利用缺乏长远的考虑，基本处于需要一点建一点、想到一点建一点，缺乏继承性，造成了大量的重复建设和反复投资。

### 1.3 自主创新不丰富，缺少良好的信息资源开发和激励机制

同美欧的发达国家相比，目前我军在信息资源的开发利用过程中，自主创新能力还比较薄弱，特别是在计算机、通信和网络技术等信息产业核心技术领域的差距还比较大。之所以创新性不足，主要存在以下几个局限性：一是局限于现有业务。由于对新时期的军事变革缺乏认识，一些开发人员忽视了由机械化到信息化的层次转变，把信息化和无纸化办公混为一谈，一些系统开发还是完全参照旧的业务形式，还是没有脱离机械化，没有在提高部队战斗力上形成质的飞跃。二是局限于现有技术。对现有技术的依赖性强，普遍缺乏创新意识，没有将工作和学习融为一体，更不会在工作中寻求创新。三是局限于现有成果。一旦取得一点突破创新，便松懈下来，坐享其成，缺乏持之以恒和不断超越自我的拼搏精神。

## 2 抓好军队信息资源开发利用应注意把握的几个问题

### 2.1 增强组织领导，完善标准体系

首先，组织有力的权威机构是信息资源开发利用的根本保障。信息资源的开发利用是个长期复杂的工程，涉及的范围比较广，存在的难题也比较多，缺少良好的组织领导，是难以解决问题的。海湾战争后，美军为增强自身的信息系统观念，将国防通信局（DCA）更改为国防信息系统局（DISA），由它统管全军的信息系统，促进了军队信息化建设的发展。无独有偶，印空军则设立了专门的软件开发学院，该院拥有全印最优秀的软件专家，负责开发、维护空军 C4ISR 作战指挥自动化系统和武器系统的计算机软件。因此，抓好我军信息资源的开发利用，必须借助于强有力的组织机构。其次，建立完善的标准体系，是信息资源开发利用的制度保障。没有标准就没有依据和兼容，就不可能实现网络互联和信息共享，也就不可能实现一体化。因此，标准法规是影响信息资源开发利用进程的决定性因素。

### 2.2 从业务中来，到业务中去

军用软件资源开发利用的根本目的，是发挥信息资源的军事效益，为部队在未来战争中获取信息优势，提高部队的战斗力，打赢未来信息化战争。因此，在信息资源的开发利用过程中，要确保信息系统的开发应该与实际业务联系在一起，增强系统的实用性，可以从两方面入手。一是强调“从业务中来”，所有的应用系统都要以业务需求为出发点，首先从现有的比较成熟的业务模型中提炼需求，再借助于当今计算机和通信领域的先进技术，开发出可以替代或辅助现有业务的信息系统；二是强调“到业务中去”，信息资源的开发利用是一个循环往复的闭合流程，由业务到系统，是业务的升华，再由系统回到业务，是系统的应用，最终实现业务水平的提高。

### 2.3 源于业务，而高于业务

目前，我军信息化建设刚刚起步，许多传统的业务还是完全基于机械化阶段的武器装备，已经不适用于新军事变革的要求。因此，军用信息系统的

开发，应以分析现有的业务为起点，但又不能局限于现有的业务，必要时就要推倒现有的业务，重新设计，用软件体系结构来指导业务创新，用业务创新来引导体制创新。具体体现在以下几个方面：一是增强业务融合性。信息化建设的核心是信息资源的开发利用，而信息系统的集成是发挥信息资源使用效益的有效途径，也增强了业务间的相互融合；二是增强平战统一性。在信息化条件下，平时与战时界限比较模糊，许多业务既可以是战时行动，也可以是平时行为，这决定了军队平时的信息化建设，必须着眼战时需求，坚持平战一体。三是增强机制创新。目前，信息资源的整体效益不高，症结在于机制的改革滞后于信息资源的开发利用，在机械化条件下形成的运行机制已经过时，只有保证我军的现行机制适应信息化的发展，信息化的成果才能发挥作用。

## 3 我军信息资源开发利用的发展趋势

当前，世界大多数国家均在不同程度地开展军队信息化建设，各自的进度快慢不一，信息资源开发利用的程度和规模也各不相同，但仔细研究对比，不难发现其中的规律所在，结合我军的当前现状，总的来看有以下发展趋势。

### 3.1 系统一体化程度不断提高

当前，各国军队都非常重视发展军事信息系统，并不断整合信息资源，提升他们的一体化程度。美军是发展军事信息系统的“领头羊”，20 世纪 90 年代初建成了一体化 C3I 系统，1996 年建成 C4I 系统，1997 年提出到 2010 年建成 C4ISR 系统，2001 年又提出到 2030 年建成 C4KISR 系统。俄军指挥自动化系统的发展方向是，将 C3I 系统建成 C4ISR 系统。

发展信息化武器装备体系，特别是军事信息系统，之所以得到各国军队的如此追捧，得益于近几场高技术战争的经验，拥有完备军事信息系统的一方，由于夺得情报和信息的控制权，战场对其几乎“单项透明”，所以能轻而易举地打败对手。因此，可以预见，未来我军的系统集成能力和一体化水平，都将不断提高。

### 3.2 系统架构设计不断成熟

在新军事变革初期,有一种意见认为,建设信息化军队是一项前无古人、需要几十年才能完成的开创性军事大工程,因而不可能制定出目标明确、步骤清晰、措施得力的严密的系统架构设计。但随着军队信息化建设的不断深入,人们逐渐认识到对系统进行顶层架构设计的重要性,各国军队开始制定和颁发相关顶层架构设计文件。美国国防部1996年和2000年分别颁发了《2010联合构想》和《2020年联合构想》,1993年、1997年和2001年先后公布了三版《四年防务审查报告》,2002年和2003年分别制定出《国防部训练转型战略计划》和《国防部转型计划指南》,2004年又制定出《DOD体系结构框架》等等。

从以上事实可以看出,做好系统架构的顶层设计,对推进信息化进程的顺利进行有积极的指导作用。军队信息化的顶层架构设计需要注意以下两点:一是短期目标和长远规划的统一。长远规划主要是指对未来军事发展趋势和变化的描述,有很强的预测性和不确定性;短期目标比较具体,其内容明确、详细,主要包括要求贯彻的建军和作战原则,以及计划开发的军事技术和信息化武器装备等。二是时效性和连续性的统一。在不断推进信息化建设的过程中,随着时间的考验,早期制定的规划难免会出现漏洞,失去指导意义,因此,对于系统的顶层架构设计,应该每隔几年修订一次,维护其良好的实效性和连续性。

### 3.3 军事理论创新不断加快

影响军队信息化进程的因素很多,除了信息化武器装备体系、新型高素质军事人才和全新的体制编制外,还包括创新性军事理论这一思想武器。创新军事理论,作为军队信息化建设的内在要求,它可以指导整个信息化进程的快速推进。自新军事变革开始以来,各国对信息时代的军事理论进行了大量探索研究,提出了很多新名词,如信息威慑、信息保护伞、第四代战争、第六代非接触战争、导航参考文献(略)

#### 作者联系方式

通信地址:山东烟台市二马路188号海军航空工程学院控制工程系304教研室

邮政编码:264001

联系电话:0535-6635690

战、信息战、网络中心战、行动中心战、全方位高级作战、凝聚式联合作战等等。目前,新军事变革已经进行了一段时期,发展到了一个新的阶段,关于如何制定下一阶段信息化建设路线,将会成为下一阶段理论创新的突破点,引领更多新概念和新观点产生。

### 3.4 技术创新带动体制创新渐成主流

实现机械化到信息化的转变,是军队信息化建设的首要任务,需要把机械化军队的组织体制逐步改造成信息化军队的组织体制,使信息可以穿梭在不同的平台和网络间,在军队内部快速、高效地流动,以适应打未来信息化战争的要求。但是,到目前为止,军队组织体制的发展变化还远远落后于信息化建设的需要,还停留在理论研究、纸上谈兵的水平。因此,在不久的将来,技术创新带动体制创新将成为时代的主流。一是军队规模的不断缩小。随着信息化时代的推进,人员数量对战场平衡的影响已经微乎其微,取而代之的将是一系列自动化的智能装备。二是军兵种结构的不断优化。提升海军和空军的比例,彻底改造陆军;组建现役与预备役兵力混编的一体化部队,在非关键岗位上编入非军事人员,都将成为可选方案。三是部队编制的不断调整。使部队的编制向一体化、小型化和多功能化改进,进一步适应信息化军队的建设。四是将创建新的军兵种部队。随着战场领域的不断扩张,一些诸如天战部队、信息战部队等新的军兵种部队也会应运而生,进一步增强部队的专业化水平。

## 4 结束语

建设信息化军队是一个规模庞大的系统工程,在开发利用好信息资源的同时,还应注重信息化人才的培养、信息化环境的建设以及信息安全等问题的解决。总之,我们只有对信息化建设有着系统的认识,并根据具体情况,采取相应的有效措施,信息化的成功建设才能有所保障。



# 军队信息化顶层设计对策分析

李贤玉 王华 贺晖

**摘 要：**在明确军队信息化以及顶层设计涵意基础上，本文简要阐述了美军信息化顶层设计的主要内容，辩证分析了我军信息化顶层设计在全面规划协调、落实法规与标准、不断创新理论、明确途径与方法、推进资源建设和注重信息化测评等方面应采取的对策。

**关键词：**军队信息化；顶层设计；对策

## 1 概述

### 1.1 军队信息化

信息化是指在社会活动的各个领域广泛运用信息技术和信息收集、传输、储存、处理设备以提高生产力与活动效率的过程。军队信息化是在军队活动的各个领域都广泛利用信息收集、传输、储存、处理设备以提高军队活动效率和满足军事指挥机关指挥员信息需求的综合性组织过程。军队信息化由军用信息技术、军用信息资源、军用信息网络、信息化武器装备、信息化人才、信息化政策法规和标准规范等六大要素构成。

军队信息化建设的目标，就是要充分利用以信息技术为核心的科学技术，建设信息化军队，实现军事形态的信息化，提高信息化攻防作战能力，打赢信息化战争；不但要实现军事人员、武器装备的信息化，而且要实现军队组织编制、军事活动的信息化。军队信息化的任务主要包括作战指挥一体化、战备响应实时化、武器装备信息化、后勤保障信息化、教育训练信息化以及军队管理信息化。

### 1.2 顶层设计

军队信息化建设全局性强、涉及面广、工作量大，需要有力与有效地加以协调。

军队信息化顶层设计是指从军队建设全局出发，由权威机构对军队信息化建设的组织领导、目标途径、理论研究、武器装备系统发展、编制体制和人才培养等进行统筹规划与指导。军队信息化建设顶层设计主要包括规划信息化建设的全局性方案，并制定相关的法规标准。

要深刻认识信息化建设对作战能力提高的牵引作用，积极探索我军信息化建设的基本规律，认真借鉴军内外信息化建设的经验，切实做好顶层设计和宏观布局，用以指导和规范各军兵种、各业务领域的建设，确保信息化建设的一体化发展；同时，要根据国内外军事环境的变化，适时更新总体发展规划，以保持顶层设计的先进性。

## 2 美军信息化顶层设计

美国军队信息化的顶层设计，体现在国防部（包括参联会）和军种部的“构想”、“四年防务审查”和“军事转型”等类型指导性文件。美军信息化顶层设计主要有五项内容。

1) 预测未来的挑战和机遇。军队信息化建设是一项长期的战略任务；要完成这项任务，必须对未来国际安全战略形势进行预测，准确把握将要面临的挑战和机遇。

2) 明确军队的任务和关键作战能力。针对目前及今后一段时期的军队任务，美军在近期信息化建设中着眼于提升六种关键作战能力，即保卫美国本土和海外基地免受大规模杀伤武器攻击的能力；有效地实施信息攻击和保护己方信息系统安全的能力；持续地实施侦察、监视和快速交战，使敌人无处躲藏的能力；强大的空间作战能力，包括空间进攻和空间防御能力；信息共享和端对端的指挥、控制、通信、计算机、情报、监视与侦察能力。

3) 创新战争和作战理论。美军的各类信息化顶层设计文件中，都包含许多创新性战争和作战理论，如网络中心战、信息行动、凝视式联合作战、非对称作战、快速决定性作战、基于效果作战等。

4) 确定军事转型的目标、内容和领域。为推

行军队信息化建设,实施军队信息化改造。这就要求实施作战方式的转型、作战组织方式的转型,以及国防部工作机制、装备采办机制、与政府其他机构合作方式的转型。

5)掌握军事转型的主要方法。美军信息化顶层设计文件确定了“远近结合”、“三种步伐”、“螺旋式发展”、“循序渐进”以及“虚拟实践”等五种军事转型方法。新编制和新装备的验证主要是在作战实验室的“虚拟实践”中进行。

美军信息化顶层设计具有前瞻性、探索性、开创性、多元性、实践性和发展性。

### 3 顶层设计对策分析

我军信息化的发展与国外先进水平存在差距,主要包括偏重于硬件建设,软件开发和信息建设明显滞后;核心技术开发能力薄弱,关键硬件和软件依赖进口;信息资源开发相当不足,而网络和数据库又存在大量低水平的重复建设,且难以实现互联和共享。

我军信息化建设必须坚持新型战斗力标准,着重进行以一体化信息支持能力为核心的信息系统建设,以信息化火力打击能力为核心的武器装备信息化建设,以多层次信息作战能力为核心的信息对抗建设,以信息系统防护和信息安全保密为主的全方位综合防护能力建设。为实现这四项能力,应强化我军信息化顶层设计,积极采取以下对策与措施。

#### 3.1 全面规划协调

在由主要领导和多种领域、多门学科的专家组成的信息化领导小组领导下,采用从定性到定量综合集成方法,对信息化建设进行总体分析、总体论证、总体设计、总体规划、总体协调;并通过由上而下-由下而上-由上而下方法集思广益,群策群力,系统谋划与协调。

应制定我军信息化建设总体发展战略,对信息化建设的长远方针进行科学筹划,指导各项工作的有序展开,并且制定信息化发展目标,对未来十年的信息化建设进行详细规划。在信息化建设中,要建立合理的体制编制、运行机制和相适应的组织结构,确保总部组织落实、指导协调和审批验收功能的充分发挥,确保各军兵种及战区信息化建设的顺利进行。

#### 3.2 落实法规与标准

军队信息化政策法规和标准规范是军队信息化建设的重要保障,主要用于规范和协调军队信息化各要素的关系,指导信息化建设的实施。在军队信息化建设的各个方面和各个环节,建立科学、实用的政策法规与标准规范,形成系统配套的信息获取、信息交换、信息发布、使用和安全保密法规制度,信息化武器装备建设法律法规和标准规范等。

信息化建设的政策法规,要符合国家的有关政策法规要求,并充分反映我军装备信息化建设的实际,适应信息化战争的需求。应组织拟制军队信息化建设技术标准、规程协议,统一各种信息系统和网络技术标准,规范各部门信息化建设活动,逐步形成科学统一的标准体系。应统一诸军兵种指挥信息系统的操作平台和技术标准,如软件与硬件平台的标准化、内外部环境接口协议的约定、信息转换标准、信息资源的标准化等,以能够真正达到诸军兵种部队间整体兼容、互联互通。信息化标准体系主要由信息技术基础标准、信息资源标准、网络通信标准、信息安全标准、应用及管理标准等构成。

#### 3.3 不断创新理论

军队信息化建设需要先进的军事理论作指导。先进作战理论的指导是形成信息化战争认知域优势的关键环节;在战争实践中创新作战理论,用新的作战理论指导新的战争实践。

要把握信息化战争的特点和规律,研究和发展具有我军特色的信息作战理论。创新信息化战争的作战形式,探讨联合作战的新样式和新内容,研究电子战、网络战的新思路;创新信息化战争的战法,寻找在非对称条件下以劣胜优的新对策;继承和创新我军的装备信息化发展理论,根据作战任务与立足现有装备,加强不同作战样式、不同作战行动、不同作战时节的信息化战法研究;紧紧围绕信息作战力量生存、信息体系对抗、信息网络安全防护等问题,寻求有效对策,不断提高我军信息制胜能力。

注重创造宽松的理论研究环境,提倡创新思维,鼓励新观点、新思想、新理论、新概念的提出,并通过“虚拟现实”等先进技术手段进行评估检验和完善,逐步形成“提出作战概念→开发新技

术及信息化装备→进行试验检验→用于战争实践”的战斗力生成机制。

### 3.4 明确途径与方法

为保证军队信息化建设阶段性目标的顺利实现,应在顶层设计中明确转型途径与建设方法。在信息化建设中,实施以信息为核心的综合集成,通过联合、整合、嵌入、附加、链接等方法,优化军队结构及各作战平台之间的组合方式;并借鉴外军“远近结合”、“循序渐进”、“螺旋式发展”等途径,以实现军队信息化建设的高效发展。

通过应用信息技术,采取软件升级、技术嵌入和硬件转换等方法加快对现有装备的信息化改造。通过信息技术的嵌入,新增或提高机械化装备的各种信息功能,在技术上与信息化装备实现接轨;通过信息技术的整合,链接或兼容机械化的武器装备系统,在体制上与信息化系统实现融合,逐步实现信息化作战要求。通过嵌入信息安全保密技术,提高信息系统的安全性及可用性;统一信息接口规范,提高信息系统的“三互”能力。

### 3.5 推进资源建设

准确、及时的信息则是夺取信息化战争主动权的关键。因此,要把信息资源规划、开发与利用作为军队信息化建设与顶层设计的重要内容。

在信息化建设中,设备、网络建设是必要的,数据库、知识系统的建立则更为重要。对预警探测、情报侦察、电子战系统等所获取的信息,应按照国家建模及信息格式标准传至信息融合中心,经加工处理和融合后供各军兵种使用,并保证信息的及时性、完整性、准确性。信息系统应以完整的知识系统为基础,具体表现为作战概念清晰、信息流程合理、数据简洁、功能实用、系统性强、标准化程度高;数据和信息集成是实现信息系统一体化的关键;要采用信息建模、数据库系统互连与集成等

参考文献(略)

#### 作者联系方式

通信地址:北京市清河大楼子九第二炮兵装备研究院第四研究所  
邮政编码:100085  
联系电话:010-66345350 010-66345341 13366839044

关键技术进行数据和信息集成,将系统中的各类数据进行合理规划和分布,为用户提供统一界面,以达到信息共享与融合的目的。

### 3.6 注重信息化测评

信息化建设既有远期目标,也有近期目标,对相关要求及指标就应给予验证和测评,因此、建立信息化测评体系是完善军队信息化建设和顶层设计内容的重要环节。对军队信息化建设进行测评和分析,不仅可以反映出军队信息化建设水平及其差距,还可以发现其中的薄弱环节及存在问题,从而分析提出解决问题的对策,并依此制定信息化发展战略。

军队信息化测评指标体系应既要满足对军队信息化当前测评的需要,又要符合预测军队信息化未来发展的要求。军队信息化测评指标体系分为测评目标、测评指标等层次,其中包括信息化实力、信息化应用、信息化能力和信息化潜力等一级指标;其中信息化实力指标侧重对基础信息化建设情况进行评估,信息化应用指标侧重测评实力指标中的各种信息资源的应用情况,信息化能力指标侧重测评信息化建设在作战指挥、后勤保障能力上取得的效果,信息化潜力指标侧重对信息化建设的重视程度、经费投入、科研能力等因素的评估。

总之,要在现有军队信息化和信息系统建设成果的基础上,根据新时期军事建设规律,着眼未来信息化战争需要,强化信息化顶层设计,在全面规划与协调、落实法规与标准、不断创新理论、明确途径与方法、推进资源建设以及注重信息化测评等方面采取实际措施,坚持以人为本,以信息技术及其成果应用为动力,以信息网络为基础,以军队指挥信息系统为核心,做好信息安全防护,以努力实现军队信息化建设的跨越式发展,实施信息一体化的联合作战,打赢高技术条件下的信息化战争。

# 信息化战争条件下空军作战对后勤保障的要求

高原 李雪娇

**摘 要：**本文深入分析了信息化战争条件下空军作战面临的新问题、新特点，在此基础上，着重阐述了为适应空军作战的新变化、新需要，空军后勤保障在信息技术保障能力、保障模式、保障手段、保障人员素质等方面的新要求和应采取的措施。

**关键词：**信息化战争；空军作战；空军后勤；后勤保障

信息化战争条件下空军作战是以信息技术为核心，以信息化的作战力量和武器装备为战争工具，在多维空间进行的战争。其作战思想、力量构成、对抗方式、战场形态等方面与机械化战争相比发生了质的变化，对空军后勤保障产生了革命性的影响，提出了全新的要求。

## 1 必须提高信息技术保障能力

在冷兵器时代，由于科学技术不发达，战争中主要是交战双方人畜体能（生物能）的直接对抗，战争是体能的战争、军队是体能的军队。此时，后勤保障主要以保障粮草为主。火药、机械制造等科学技术的发展及其在军事领域的大量应用，使战争进入了热兵器时代，战争中主要是交战双方热兵器的对抗，战争是热能的战争，热能是通过士兵的技能和指挥员的指挥才能释放的。因此，热兵器时代的战争是技能战争，部队也是技能部队。此时，后勤保障主要以供应弹药、油料和实施机械维修为主。

20 世纪 60 年代末以来，以计算机、微电子、遥感遥测和通信为主的信息技术的迅速发展及其在军事领域的应用，不但使信息技术与传统武器装备相结合，产生了信息武器及信息武器系统，而且使信息本身成为武器（如计算机病毒），并随着信息技术的进一步发展，已经或即将出现数字化部队和数字化战场，信息武器时代已悄然到来。战争中主要是交战双方信息、信息武器和信息武器系统在数字化战场上的对抗，各种武器的能量都是在智能系统产生的指令信息控制下释放出来的，且运动着的信息本身也带有能量。因此，信息武器时代的战争是信息战争或信息化战争，军队是信息化军队或智

能军队。由此也可看出，在信息化战争中，空军作战主要依赖于信息源，争夺制信息权的斗争将异常尖锐、激烈。如果说，机械化战争空军作战打的是钢铁和能量，信息化战争空军作战打的就是信息。没有信息，空军作战部队就成了“瞎子”、“聋子”。可以这样讲，制信息权，渗透在信息化战争空军作战的各个领域，贯穿在作战全过程，是双方争夺的焦点。因此，空军后勤保障活动必须紧紧围绕制信息权而展开。具体来说，就是信息化战争空军后勤保障，要与信息化作战平台相融合，提供其相应的保障物资和技术服务；着眼于信息化战争条件下空军作战物资消耗大的特点，应该增大信息化物资器材和装设备的数量；根据信息化战争条件下空军作战行动的进程和节奏，及时提供精确的后勤保障物资。

在战场范围广，部队机动快，保障需求变化大的情况下，掌握信息对于空军后勤保障更加重要，制信息权就是保障工作的主动权。从发展趋势看，空军后勤要掌握制信息权，主要是利用计算机技术、网络技术和自动识别技术，建立信息化平台、数据库系统和后勤指挥自动化系统，实现对所有保障资源、保障需求的动态可视，实现对所有保障活动的有效控制，组织适时、适地、适量的精确化保障。这是信息化战争条件下空军作战后勤保障的核心。

## 2 必须实现多样化和高效化

信息化战争，非接触、非线性作战将成为空军的主要作战样式。随着科学技术特别是信息技术的飞速发展及其在军事领域的广泛应用，加快了武器装备更新换代步伐，并实现“质”的飞跃，促使作

战形态相应发生新的变化,敌对双方将在全纵深范围内进行非接触、非线式的立体机动作战,远程精确打击成为主导作战样式,战场空间由平面到立体到太空、由三维到四维到多维,空军后勤传统的保障方式已难以适应未来信息化战争空军作战需要,必须实现由静态式固定保障向动态式机动保障转变,由平面式单一保障向立体化多维保障转变,由军队自我保障向社会化网络保障转变,由垂直式逐级保障向越级式直达保障转变。

机械化战争条件下空军作战后勤保障主要依托补给基地,实行划区、定点和逐级保障。主要特点是:以平面为主,以线式为主。信息化战争条件下空军的精确打击能力、机动突击能力不断提高,作战不再是从前沿到纵深逐线突破,逐步推进,而是超越时空,直接攻击纵深目标,在非接触的状态下速战速决。非线式、非接触作战,战场范围空前广阔,前后方界线、攻防界线变得越来越模糊,要求空军后勤保障必须多样化和高效化,真正实现保障过程能够随战场形势和作战行动、作战需求的变化,准确掌握和调控后勤资源的流向流量,实现物资供应保障的适时、适地、适量。因此,空军后勤要在动态中准确定位,在机动中寻求优势,机动保障和立体保障的地位越来越重要。空军后勤保障必须依托信息技术和多种投送手段,在多维空间,组织立体、远程、快速的机动保障,这样才能取得保障工作的主动权。海湾战争中,美军投入 600 多架战略运输机,组织了历史上最大规模的远程立体快速投送,向作战地区运送 52 万部队,610 万吨油和 400 万吨其他物资,有效地保障了作战需求。阿富汗战争中,美军空中投送的兵力达到 90%。这都说明,在多维空间的机动、立体保障能力,已成为衡量空军后勤现代化水平的重要标志。

### 3 必须实现集约化和一体化

信息化战争条件下的空军作战行动是三军一体的联合作战行动,即使是以空军为主的空中作战行动也必须有其他军种的密切配合。从作战力量的构成上看:信息已成为未来战场的主要资源和取得战争胜利的基础,夺取信息优势是未来信息化战争追求的首要目标,而参加信息作战行动的既有三军信息作战的专业部队,又有装载在机、舰、弹等武器系统上的自卫信息对抗设备,既有军队的信息作战

力量,又有地方的民兵、预备役信息作战力量,使得信息化战争的作战力量的构成呈现多元化,参战力量的多元化要求保障力量必须多元化;从信息化战争的作战行动上看:信息化战争中各作战单元、各武器系统都是通过信息系统的粘合作用而凝聚成一个作战整体,失去了这种粘合作用,各种作战力量就成了一盘散沙,而要充分发挥各种作战武器的综合作战效能,则必须紧紧围绕总体作战企图,在联合作战指挥员的统一指挥下,按统一的作战计划有序联合展开,并且保持战役的最高指挥机构不仅能在广阔的战场空间范围内实时控制各军兵种,而且还能控制到各军兵种的某个武器或作战单兵,使信息化战争中的战场情报、指挥、控制、通信、打击、毁伤评估等各种职能,集约成一个有机的整体。信息化战争的这种力量编成的高度集约化、作战指挥控制的高度一体化,必然也促使后勤保障的一体化和集约化。一方面,一体化、集约化的后勤保障,将在现有联勤保障体制基础上,进一步打破军种后勤保障的界限,从全局上优化配置和使用后勤保障资源,这样可以提高各军种后勤保障资源的使用效率,避免重复浪费,从而提高整体保障能力和后勤保障效率,使后勤保障与一体化的作战行动相适应;另一方面,在数字化的战场上,信息纽带不仅把诸军兵种的后勤力量、地方民用后勤保障力量连为一体,而且把各军兵种、地方保障力量的保障行动连为一体,这就为信息化战争中空军作战实施诸军兵种一体、军民一体化、集约化的后勤保障创造了条件。

### 4 必须实现精确化和快速化

随着信息化、智能化的武器装备在空军作战中的大量应用,使得信息化战争空军作战行动的机动速度加快、持续时间缩短、打击的精度提高。为适应多维空间、全纵深地域作战,空军作战武器装备的机动速度、距离将大幅提高,同时在数字化的战场上借助于信息网络可随时获取作战信息、进行实时处理,并立即定下作战决心,采取相应的行动;超视距、全方位、多维空间的信息化打击手段,使空军武器装备的打击精度进一步提高,对敌方系统要害部位实施精确打击后,往往很快会迫敌就范,战役行动的持续时间很短。正是信息化战争空军作战行动的这些特点,使得空军后勤保障的难度进一

步加大,为了适应瞬息万变的战场形势变化,要求空军后勤保障必须实现精确化、快速化。一方面,信息化战争空中战场形势瞬息万变,要求空军后勤必须在规定时间、地点提供准确的保障。首先,信息化战争空军作战非常注重时效性,战争进程快、时间短,因此,对后勤保障的时效性要求空前提高,要求空军后勤必须在准确的时间进行保障;其次,信息化战争空中战场是高度立体化的非线性战场,部队机动能力的显著提高和运动速度、范围的空前增大,对空军后勤实施保障地点的准确性要求提高,要求空军后勤必须在准确的地点进行保障;再者,信息化战争空军作战物资消耗巨大,而物资储备却相应下降,因此,对保障物资的品种及数量的精确性要求提高,要求空军后勤必须有相应品种和数量的物资进行保障。

另一方面,信息化军事技术的发展为军队后勤保障特别是空军后勤的精确性提供了可靠的物质和技术基础。信息化战争空军作战部队由于拥有先进的空中和地面侦察器材和手段,以及各种信息传输与处理设备,其获取和运用信息的能力空前提高,可实时地获取战场上敌我双方的各种信息,尤其是己方作战的各种信息,因此,对空军部队作战的地点、进程、规模及物资消耗和对后勤保障的需求均可及时精确地掌握,并且无缝隙实时地了解物资的生产、储备、运输信息,这些都为空军后勤保障的精确化奠定了牢固的信息基础。总之,根据信息化战争条件下空军作战行动“信息流”,控制空军后勤“物流”的流向、流量和流速,组织适时适地适量的投送,实现空军后勤保障的精确化和快速化。

## 5 必须实现保障手段的立体化

信息化战争条件下空军作战,即使是小规模作战行动,也需要部署在太空的卫星监视系统、空中预警与控制系统、联合监视与目标攻击雷达系统、无人驾驶飞机,搜集、处理和传输大量数据信息,这就使作战由机械化时代的航空作战向信息兵器时代的航空航天作战发展。信息化战争条件下,空中战场沿长、宽、高三个方向拓展,空中作战已经具有全方向、全纵深、全高度和空天一体化的性质。新世纪伊始,美国空军进行了世界军事史上的首次太空演习,大步迈开了向天军过渡的步伐;俄罗斯军队也已成立了航天兵,抢夺外层空间的战略

制高点;欧洲其他军事强国也都在竞相发展航天力量和推进空天一体化的建设。外层空间的军事化,使得空天一体化的战场已经成为信息要素显示威力和体现信息化战争特征的主要作战空间,成为以诸军兵种联合作战为主要形式的信息化战争的主导战场。信息化战争的战场空间的广延性,要求空军后勤保障空间必须要同步扩展。长期以来,空军后勤一直是地面保障方式依托机场阵地实施保障,由于空军作战的战场在空中,而后勤保障却在地面进行,这就使保障活动与部队的作战活动形成一定的空间差,在很大程度上限制了空中作战效能的发挥。因此,未来信息化战争空军后勤必须将保障方式由平面转向立体,形成在多维作战空间内实施保障的能力。

首先,由于作战力量已经突破了就地筹划的传统模式,后方很可能远离战场,因此,后勤保障必须具有远程保障能力,包括远距离投送后勤力量的能力、掌握遥远战场后勤保障动态的能力,以及组织全程保障的能力。如:运用空中医疗救护、空中加油、空中修理等手段实施后勤保障,将空中运输发展为主要的运输方式。

其次,多种高技术保障手段的综合运用,使保障场所向空中、地下延伸,为空军后勤保障手段的立体化奠定了基础。传统平面保障模式被打破,而保障空间的多维化,使保障方式更加灵活多样,保障内容更加丰富。如发展地下管线输油技术,后勤指挥、飞机停放及物资储备可转入地下。还可以利用地下工事进行飞机维修,甚至在地下进行飞行后勤保障工作。

## 6 必须实现人员的知识化

信息化战争中空军作战是借助于信息化的武器装备,通过智能化的指挥控制手段在数字化的战场上与敌进行的高技术较量,从某种意义上来说,信息化战争是交战双方的知识和智慧的对抗。众所周知,在知识经济的新时代,知识将成为真正的资本和首要的财富。同样,在军事领域,知识将是军队战斗力的核心要素。一方面,无论信息化武器,还是数字化战场,都是人的知识和智慧物化的产物;另一方面,无论信息化武器装备多么先进,作战手段多么智能化,都需要具有相应知识和智慧的人来驾驭。现代高技术局部战争用残酷现实告诉我们一

个真理：“钢铁”和“芯片”并不会自然生成战斗力，再先进的装备，没有高素质的人才去驾驭、维护、操作，就形同虚设，更难以发挥其作用。在信息化战争中，空军后勤作为一个专业门类复杂、科技知识密集的保障群体，必将大量使用科学技术含量高的信息化、智能化的后勤保障装备，而没有大批掌握高科技知识的后勤人才，就无法研制、驾驭这些信息化装备。因此，空军后勤要想在未来战争中真正实现保障有力，其关键仍取决于有没有与信息化战争客观要求相适应的高素质人才。正如美军在《2010 年联合构想》中指出的那样：“招募和保留具有献身精神的高素质人员仍是美军部队建设的头等大事。一支部队，只有其勇敢、毅力和智慧能够适应未来联合作战复杂环境时，才能拥有夺取全

面优势的能力。”美军人员文化素质已达到相当高的水平，还如此重视军事人才队伍建设，而我们空军后勤保障人员在知识结构老化，素质偏低的情况下，就更应该加强以掌握高科技知识为重点的后勤人才队伍建设，这是信息时代空军后勤建设面临的最严峻的挑战。当然，空军后勤所需要的人才不仅是指比尔·盖茨那样的个别精英，而应是一个具有聚集效应的人才群体。这个群体包括：能瞄准军队后勤保障和高新技术的发展趋势从事科研创新的科技开发人才；精通后勤保障理论和野战勤务知识，具有高超的后勤指挥艺术的后勤指挥人才；具有高深的专业知识，精湛的操作技能的各种专业技术人才；娴熟掌握高新技术特别是信息技术知识的后勤管理人才。

### 参考文献

- [1] 徐小岩主编.《军队信息化概论》.北京：解放军出版社，2005
- [2] 侯喜贵主编.《军队信息化建设研究》.北京：解放军出版社，2005
- [3] 郭炎华.《世界军事强国军队建设研究》.北京：国防大学出版社，2002
- [4] 李辉光主编.《美军信息作战与信息化建设研究》.北京：军事科学出版社，2004

### 作者联系方式

通信地址：空军指挥学院后勤与装备系后勤教研室

邮政编码：100097

联系电话：010-66924357 13671089981

# 美国临近空间发展综述

李铮 程建

**摘 要:** 本文介绍了当前美国在临近空间领域的发展状况, 分析了其发展的动因及临近空间平台的优势。介绍了美国的发展规划和正在进行的项目, 分析了临近空间平台在通信、预警探测和兵力投送的应用价值。

**关键词:** 临近空间; 近空间

## 1 引言

“临近空间”是最近备受关注的一个新概念。目前, 大多数专家倾向于把临近空间的范围定义在20~100km, 它基于多种考虑, 把20km作为临近空间的最低底界, 主要是因为它必须在国际民航组织(ICAO)控制的空域18.3km之上; 临近空间的最高界限定为100km, 主要依据国际航空联合会(FAI)的定义, 考虑已有国际空域主权的协议和惯例。

在临近空间这块特殊的空间, 这里的气温、气压和气象等环境有别于航空空间和航天空间, 牛顿万有引力定律和开普勒宇宙飞行定律在此不能完全发生作用, 航空器和航天器因而失去了随意运行的自由。临近空间特殊的物理环境, 决定了目前人类所有的航空器和航天器都无法在其间飞行。这就意味着: 临近空间的绝大部分空间, 人类只能“穿越”但无法在其间自由飞行, 因此, 临近空间就成了“空”与“天”之间的横断区。

## 2 美军临近空间发展现状

### 2.1 美军临近空间研究现状

美军认为临近空间不同于航空和航天空间, 具有承上启下的作用, 与其他平台相比具有生存突防能力强、机动性好、费用低、应用范围广等特点, 并能执行快速远程投送、预警、侦察与战场监视、通信中继、信息干扰、导航等任务, 在空间攻防和信息对抗中能发挥重要作用。2004年, 时任美国空军参谋长江柏就要求美国空间司令部尽其所能研究如何为美军提供战术级的太空作战能力, 他看到

了临近空间平台的巨大潜力, 认为: “它们能提供与空基武器相同的能力, 且性价比更高, 灵活性更强。”由于临近空间具有巨大的军事应用价值, 如今美国国防部对开发临近空间平台抱有极大的兴趣, 目前正在加速临近空间作战平台的研究。在美国空军方面, 临近空间军事应用研究由空军研究实验室牵头, 对临近空间平台、有效载荷及其集成展开研究, 同时确定了临近空间飞行器的10个应用方向, 包括在全球定位系统(GPS)系统的协助下实施跟踪、侦察和情报搜集等。目前, 临近空间飞行器虽然还处在研究、论证和试验阶段, 但由于其自身所具有的优势, 使其具备了良好的发展前景。2005年2月美军在内华达州内利斯空军基地秘密进行了“施里弗-3”太空站模拟演习中首次把临近空间的概念引入演习, 演习的重点是探讨在2020年发生的反恐战争中如何使用航天装备支援陆海空联合作战。

### 2.2 美军临近空间平台研发情况

美国、日本、以色列、欧盟、俄罗斯等为了取得临近空间的控制权, 围绕侦察监视、空中预警、通信等主要应用方向, 纷纷制订计划, 研究开发各种临近空间平台。下面, 就美国各种临近空间平台的研发情况及主要计划做一介绍。

1) 平流层飞艇。美国将其作为将来国土防空预警的主要平台予以大力发展。2003年11月, 美国空军空间作战实验室和空间作战中心的临近空间机动飞行器(NSMV)原型机, “攀登者”在30000米高空进行了初期试验和配载实验, 实现了运载45千克载荷、悬停5分钟及各种控制要求。近期, 在美国新的导弹防御计划中, 美国计划从西北部皮吉特湾开始的太平洋沿岸, 到美国的大西洋



沿岸,再到最东北的缅因州为止,至少部署 10 艘高空飞艇(HAA),用来监视来袭飞机、舰船和巡航导弹。此外,美国导弹防御局正在考虑在北极上空部署可控气球,用来监视和跟踪俄罗斯的导弹。美国进行模拟仿真的结果显示:在北纬 83 度地区 36.6km 高空上部署 3 个气球,可连续覆盖从北极到北纬 45 度范围的导弹发射;30 个这样的平台就可以提供类似的全球覆盖;800 个这样的平台组成的星座可以对全球连续提供按需通信和情报、监视、侦察(ISR)覆盖。

2) 高高空有人/无人飞机。美国将其主要用于情报侦察。“全球鹰”高空长航时无人机(RQ4A 型),飞行高度 22 千米,航程 26000 千米,续航时间 41 小时,有效载荷 1800 千克以上。

3) 平流层高空气球。美国将其主要用于科学研究。2004 年底,美国国家航空航天局(NASA)发展了长时间飞行气球,悬挂 2000 千克的科学仪器,并升至 38 千米高度,在南极点上空绕地球轨道 3 圈,飞行 42 小时后着陆。正在研制的超长时间飞行气球,预计飞行时间可达 100 天左右。

4) 太阳能平流层无人机。美国计划将其主要用于情报侦察,目前已经进行多次试验,但还没有进入实用阶段。NASA 与南加利福尼亚空间环境公司开发的 Helios(太阳神),重量约 700 千克,由 14 个无刷直流电动机驱动螺旋桨推动,动力由单晶硅太阳能电池提供,可产生 35 千瓦能量,载荷重量 100 千克,飞行高度 30 千米,先后进行了两次试飞,2001 年 8 月试飞高度 29.4 千米,飞行时间近 17 小时。

### 3 临近空间发展的主要原因

#### 3.1 临近空间发展的动因

目前,美军的航天装备发展迅猛,但是在诸多方面还是很难以尽如人意。美军 70% 以上的通信、80% 以上的预警探测、90% 以上的精确制导武器依赖航天装备。从性价比上来看,卫星设备极其昂贵,而且往往受制于带宽和实用性的局限。从操作效能上看,非同步卫星在某一地点停留的时间极短,可运用的时间稍纵即逝,如果目标区域不在轨道的范围之内,就必须重新部署,这个阶段往往需

要几天甚至是几个月的时间,根本无法保障现代信息化战争的需要。从装备能力上来看,太空中的情报通信设备,面对海量情报通信时,显得力不从心。所以,我们不难看出,正因为太空装备在局部高技术条件下的信息化战争中表现的不足,是美军大力发展临近空间的起因。

临近空间平台的既有优点是其发展的主要因素。与卫星相比,临近空间飞行器的优点是:① 性价比高,易于更新和维护。临近空间平台固有的简易性、可恢复性和不需要空间加固防护以及地面支持设备需求小等特点,构成了临近空间平台明显的成本优势。气球、飞艇等临近空间飞行器仅仅需要氦气作为上升动力,而不需要复杂昂贵的地面发射设施将其送入轨道。当临近空间平台携带的载荷出现故障时,载荷可以回收至地面进行维修,便于实现载荷的替换或者升级工作,这对于卫星平台显然是不可能的。② 分辨率和灵敏度高。临近空间飞行器距目标的距离一般只是低轨卫星的  $1/10 \sim 1/20$ ,可收到卫星不能监听到的低功率传输信号,容易实现高分辨率对地观测。③ 快速反应能力强。临近空间平台具有良好的快速反应能力。它的发射过程所需的地面辅助设备很少,一旦平台到位,就可以在数小时内迅速地建立起战区通信和预警侦察体系。

与传统飞机相比,临近空间飞行器的优点是:

① 持续工作时间长。临近空间飞行器的留空时间以天为单位,易于长期、不间断地获得情报和数据,可对紧急事件迅速做出响应,而且可以相对减轻人员保障和后勤负担。② 覆盖范围广。临近空间飞行器的飞行高度在传统飞机之上,其覆盖范围比传统飞机广。③ 生存能力强。气球或软式飞艇的囊体采用非金属材料,雷达和热反射截面很小而且低速运行,传统的跟踪和瞄准办法不易发现。

#### 3.2 临近空间平台的用途

1) 巡航导弹预警。一般来说,巡航导弹在不同地形的巡航高度为:在海面上飞行高度为 5~10m,平原地区为 15m,丘陵地区为 50m,山区为 100m 左右。可按预定程序绕过固定的防空阵地,从侧面或背面打击目标。当巡航导弹到达目标附近时,即使被发现,但时间短促,防空武器已经很难有所作为了。另外,隐身巡航导弹的出现,为地面雷达预警又增加了新的难度。巡航导弹通过采用低

RCS 外形技术、吸波材料技术等措施躲避地面雷达的追踪,实现隐身。但是隐身巡航导弹虽然隐形,但其隐形效果主要作用于前方、下方的防空雷达。因此,在空中设置多种防空传感器,隐形巡航导弹的散射能量就会在多种传感器上体现出来。这些传感器获取的信号经过处理就会得到较完整的目标信息,为拦截提供一定的时间。

然而,天基预警探测系统由于离地面太远,地表又经常被云层覆盖,不能有效地探测到低空飞行或超低空飞行巡航导弹的特征信号。目前被广泛采用的机载雷达探测虽然能有效地探测到巡航导弹目标,但由于其不能长时间工作,探测位置不固定,不能对巡航导弹进行持续有效的预警。

为了探测巡航导弹,保卫国土安全,采用临近空间飞行器预警已成为必然趋势。目前,美军已做了大量的实验,临近空间飞行器一般由轻型复合材料制成,具备良好的红外和雷达隐身能力,在其上搭载各类传感器,既可用于战区内重点目标的前沿防空,又可执行空中巡逻、环境监测等多种任务。它一方面受到防空导弹的保护,另一方面与防空导弹配合,构成一个立体防空体系;与现有预警探测系统配合,可以组成空天一体预警探测系统,使系统整体达到最优。

2) 通信中继。随着作战半径越来越大,通信内容越来越多,原有的地空通信、卫星通信已不能满足要求,临近空间飞行器既可以直接与作战单元进行通信,也可以作为卫星通信的中继平台或者地空、空空远程通信的中继平台,将远程作战单元的信息传输给地面指挥中心,或者将地面指挥中心或者其他作战单元的信息传输给另外的作战单元。临近空间飞行器用作高空中继通讯平台时,其通讯几乎不受地形条件的限制,可实现超视距通讯。覆盖范围方面:部署于 30km 的临近空间飞行器其视距覆盖直径大于 1200km,面积大约  $45 \times 10^6 \text{m}^2$ ,比普通地面无线电系统的通讯范围大一个数量级以上。指向精度方面:部署于 30km 高空用作通讯的临近空间飞行器,如果其定位精度小于 50m,则地面指向精度将小于 0.1 度,携带通信转发器后甚至可以部分代替通讯卫星的职能。临近空间飞行器与

通信卫星相比,其信号往返延迟短、发射成本极低、信号衰减小,有利于实现终端的小型化;与地面无线电系统相比,作用距离远、覆盖地区大、无通信死区,因而发射功率可以显著减少。

3) 兵力投送。2003 年的伊拉克战争期间,由于土耳其方面拒绝美军借道土伊边界从北部进攻伊拉克的要求,致使美军南北夹击伊军的计划未能实现。由此,装备与兵力的快速投送问题引起美军的高度重视。随着对临近空间研究的升温,临近空间飞行器有可能成为装备兵力投送的理想工具。

美军正在研究的一种用于装备兵力投送的重型飞艇“海象”被赋予“空中运输舰”的美称,按照设想它能越洋跨洲飞行。它既结合了空运的快捷,又兼顾了海运的大载重量,能够在 3~4 天内运送 1800 名士兵或 500 多吨武器装备,到达世界上任何地点,行程超过 11000km。2005 年 1 月,美国国防预研局(DARPA)公布了“海象”发展计划的指标征询书,6 月授予“海象”发展计划第一阶段的合同,到 2008 年将会把一架“海象”技术验证飞艇送上高空。

## 4 结论

空天一体信息作战将成为 21 世纪主要的作战方式之一,空间和空中作战的界限变的非常模糊。从美军临近空间开发情况我们不难看出,临近空间作为新的信息平台,由于其独特的环境特性,临近空间已成为陆、海、空、天之外又一新的军事应用空域并备受关注,它将成为联合作战空间的重要组成部分。凭借其突出的特点,临近空间飞行器有着广阔的应用前景。它将有效弥补军用航天器和航空器的不足,提高武器装备的联合应用能力,增强整体作战效能,成为未来联合作战中一支新的重要力量。临近空间飞行器的出现将催生新的作战样式,改写联合作战理论,并对未来高技术局部战争产生重大影响。

参考文献(略)

作者联系方式

通信地址:陕西西安沣镐东路 1 号空军工程大学电讯工程学院 14 队

邮政编码:710077

联系电话:13488184685

# 航天测控技术发展及我们的对策

李志强 张应宪

**摘 要:** 首先分析总结了国际航天测控发展的三个阶段与七大发展趋势。在此基础上, 分析了国内航天测控的现状, 提出了我国航天测控的发展对策, 最后总结全文。

**关键词:** 航天测控; TT&C; 卫星测控; 测控通信; 趋势

## 1 引言

随着“神舟”载人飞船的成功发射、“嫦娥”探月工程等一系列航天活动的开展, 我国的航天事业进入全新的加速发展时期。在国际上, 各国从对于建立各自的卫星通信系统到进行深空探测也都进行得如火如荼。如果把各种航天器比做“风筝”, 那么航天测控就是牵引这风筝的“线”! 它是保证一切航天活动成功的基础。

本文首先简要回顾了航天测控发展的三个阶段, 总结了国际航天测控发展的七大发展趋势, 然后分析了国内航天测控的现状, 提出了我国航天测控的发展对策, 最后是全文的总结。

## 2 国际航天测控发展趋势

### (1) 航天测控发展的三个阶段

测控的英文原为 Tracking Telemetry & Command, 即轨道跟踪、遥测与指令, 简写为 TT&C, 在国内统称之为测控。航天测控的发展, 经历了以下三个发展阶段。

#### 1) 分离测控体制阶段。

20 世纪 50~60 年代, 跟踪、遥控和遥测是相互分离的, 三个系统拥有各自的空间段和地面段, 每个系统具有独立的收发天线、收发信机与调制解调终端。三者相互配合工作, 设备庞大负责, 相互还存在干扰等问题。

#### 2) 统一载波测控体制阶段。

20 世纪 60 年代至今, 是统一载波测控体制广泛使用的时期。统一载波测控体制只用一个上行和一个下行载波解决了测距、测速、测角、遥控、遥测等所有问题, 而且收发天线、伺服系统、发射

机、接收机都统一为一套, 大大提高了测控的效率, 故沿用至今。

#### 3) 通信与测控结合时期。

20 世纪 80 年代以后, 航天器作为承载仪器的空间平台, 开始转入应用阶段, 获取和中转信息成为主要目的, 因此对航天器而言, 通信和测控是必备的两种手段, 这促进了通信与测控的融合。通信和测控共用载波的调制方式, 在美国的跟踪与数据中继卫星系统 (Tracking and Data Relay Satellite System, TDRSS) 中开始采用, 在本世纪将会得到推广。这也是航天测控的发展趋势之一。

### (2) 航天测控发展的七大趋势

1) 采用扩频测控体制由单站单星测控向多站多星测控转变。

现有的统一载波测控系统是采用副载波调制的频分系统, 遥控信号、测距信号、遥测信号分别调制在不同的副载波上, 然后再调制到统一的载波上, 不同分系统共用一个载波频率和信道设备。

由于统一载波测控系统靠点频区分不同目标, 多星同时测控需要多套相似的设备同时工作, 设备重复浪费严重。同时不可避免地存在各点频之间的互相干扰问题, 解决起来非常困难。因此当需要测控的卫星数量越来越多, 频率资源的紧张无法缓解。

在需求方面, 随着国家实力的增强, 在轨卫星数目的不断增加, 很多卫星尤其是小卫星往往需要组成星座或者编队飞行以完成特定的任务, 因此一个测控站管辖的空域范围内可能同时出现多颗卫星需要进行测控的, 于是就要求测控站具备能够对本站空域内的多个目标进行跟踪、定位、遥控和遥测的能力。

因此, 为解决上述矛盾就需要测控站从传统的

单站单星测控模式向多站多星测控模式转变。解决办法是采用扩频技术和 CDMA 技术,即统一扩频测控体制。

目前国际上对航天器的测控越来越多地应用了扩频测控技术。如目前运行的 Globalstar 系统就采用了扩频测控技术,欧洲的 ESTI EN 301 926 V1.2.1 标准规定了欧洲地球同步轨道卫星遵循的扩频测控体制技术规范,典型的美国跟踪与数据中继卫星系统(TDRSS)中也采用了相干扩频测控技术。采用这种机制,可以将扩频技术和加密技术结合,实现卫星通信和遥测信息的加密,提高了卫星的安全性和抗干扰能力。采用扩频机制还具有组网简单灵活、系统容量大、成本低等一系列优点。

## 2) 从地基测控向天基测控转变。

近代航天测控通信技术的重大突破是天基测控通信网 TDRSS 的建立,“天基”的设计思想从根本上解决了测控、通信的高覆盖率问题,是解决多目标测控的可行途径之一。

“跟踪与数据中继卫星系统”是一个利用同步卫星和地面终端站,对中、低轨卫星(称为用户航天器)进行高覆盖率测控和数据中继的测控通信系统。这个系统中的同步卫星称为跟踪与数据中继卫星,因为它从远离地球 3.6 万公里的同步轨道向地球俯视,所以覆盖范围很大。这可形象的视为把测控站搬到了天上的同步轨道,故又称为“天基测控系统”。

TDRSS 可进行多目标测控通信,目前美国的 TDRSS 能对 24 个用户星同时进行测控通信,其多目标测控通信的方式为 TDRSS 生成多个波束分别对准不同的用户,从而实现多目标同时测控通信。

对于低轨道的飞行器,如大量小卫星,距 TDRSS(同步轨道)的最远距离比距地面的距离远得多,所以要达到相同的测控和数传指标,在应用 TDRSS 时,低轨道的飞行器上需要更高的 EIRP 和 G/T 值。为了解决这个问题,美国研制了第四代应答机用作小卫星测控,该应答机的特点是:① 采用了 K 频段以提高 EIRP 和 G/T 值,并具有 K 频段小型相控阵天线,用于通过 TDRSS 传输小卫星的数据;② 高集成度的高频和数字电路以减少部件数量;③ 降低接收机和发射机功耗;④ 采用 CCD 信号处理技术降低了成本,体积和功耗。目前该应答机还处于验证阶段,其成功应用将成为 TDRSS 系统实现低轨多目标测控管理的标志。

## 3) 测控与通信从分离向融合转变。

目前,无论统一载波测控体制还是统一扩频测控体制,飞行器的测控分系统与通信分系统都是分离的,即各自完成自己的任务互不相关。然而,测控与通信在本质上并没有太多的区别,只是侧重点不同,完全可以将测控与通信结合起来,这对于减小飞行器的体积、重量,充分发挥飞行器有限的功率资源都具有重大意义。

更高的测量精度和更高的数据传输速率是测控系统追求的目标。综合数字基带技术将测控与通信有机结合起来,使得上述目标变为可能。

## 4) 军用卫星测控向具有抗干扰和抗截获能力转变。

军用卫星处于纷繁复杂的电磁环境中,面临的各种干扰日益严重,它的安全问题直接涉及航天器的可用性和生存能力。因此,空间信息对抗就要求军用卫星必须具有抗干扰和抗截获能力。

对于军用卫星而言,对扩频测控系统主要干扰威胁是敌方人为干扰。通常的人为干扰主要有如下几种:阻塞式噪声干扰、窄带干扰、单音连续波干扰、宽带相关干扰等。

统一扩频测控体制采用 DSSS 信号进行传输,将有用信号和干扰信号频谱能量都加以扩散,在接收端利用 PN 序列的相关特性进行相关处理,对有用信号频谱能量压缩集中。干扰和噪声因与 PN 码不匹配而被抑制,因此大大提高了信噪比,天然具有较强的抗干扰能力,因此是发展的方向之一。除此之外,对于有意或者无意的窄带干扰,通过先进的干扰消除技术可以达到很好的效果。。

在系统设计上,信号的抗截获和信息的抗截获都是必须考虑的问题。DSSS 信号在低功率谱密度下传输,有用信号功率比干扰信号功率低得多,信号仿佛淹没在噪声之中,具有较强的防截获能力。另外,DSSS 信号采用 PN 码调制,不掌握发射信号的 PN 码规律,要进行解扩是很困难的。这些都体现了扩频测控体制安全、保密的特点。

采用非线性序列,如混沌扩频序列,甚至无周期扩频序列是提高 DSSS 抗截获能力的重要途径。在测控信息设计上的独特性是提高信息抗截获的有效途径。

## 5) 测控频率向更高频段转变。

目前卫星测控体制使用的测控频率主要有两种,一种是 S 频段统一载波测控 USB(Unified S

Band) 体制, 一种是 C 频段统一载波测控 UCB (Unified C Band) 体制。欧洲的 ESTI EN 301 926 V1.2.1 标准规定了欧洲地球同步轨道卫星遵循的扩频测控体制技术规范, 其测控频率除了常用的 S 频段和 C 频段外, 还使用了 Ku 频段。美国下一代的测控应答机也使用了 K 频段。

测控频率向更高频段发展, 目的是为了使得飞行器获得更高的 EIRP 和 G/T 值, 从而进一步提高测量精度和增强抗干扰性能等。

6) 星座卫星测控向具有自主管理能力转变。

星座系统一般着眼于小卫星系统, 小卫星系统的成本一般比较低, 从卫星技术的发展看完成用户所赋予的任务不存在技术难度, 且相对于大卫星而言功能相对单一。星座内卫星具备一定的自主管理能力, 一方面是小卫星技术发展的趋势, 另一方面从一定程度上可以提高系统费效比。提高卫星的自主管理能力, 可通过星座内卫星的自主管理、利用国内或国外的自主导航定位系统、卫星间具备星间链路功能等方式简化测控要求, 降低卫星地面测控操作管理费用, 卫星自主管理的相关技术已在我国小卫星技术中得到成功应用。

(a) 卫星故障的自主诊断与处理。如我国的试验一号卫星就是采用基于故障检测、故障处理与系统重构的管理方法。卫星的自主管理主要依赖于星载计算机。首先, 星载计算机系统须具有灵活的系统重构能力, 故障检测及故障处理主要由卫星自主进行, 在检测到故障后, 根据系统资源再进行系统重构。地面测控管理仅作为系统资源在重构过程中不足以构成完备控制模式时, 确保卫星进入安全控制模式的一种手段。

(b) 星地协调统一的接口设计标准。目前, 有关这方面的行业标准国际、国内都有详细规定。具体说, 根据任务阶段可以采用分包遥测方式选择相应的遥测参数发送到地面, 且仅发送与此次控制目的有关的信息, 这可限制申请地面测控管理的次数; 也可以根据需求采用分包遥控方式仅进行与控制目的有关的上行操作, 而无需进行繁琐的大量的数据注入。

(c) 采用星际链路。使用象“铱”系统星座内控制卫星所用的星间链路。目前为止, 根据我国航天技术的发展状况看, 目前选用星间链路可能会增加系统的设计难度, 需要攻克卫星平台、卫星天线等一系列问题。

(d) 使用卫星自主导航技术。可以利用国内或国外的自主导航定位系统, 国外可供利用的手段有 GPS、GLONASS 等系统, 国内可利用的有北斗一号导航定位系统和在建的北斗二号、中继卫星系统等。航天器采用自主导航技术, 可以减少地面频繁的测定轨和参数注入, 大大简化了地面测控管理的次数。

7) 利用其他静止轨道卫星完成测控任务。

TDRSS 系统的出现解决了多个卫星同时测控与地面站数目有限之间的矛盾。近年来, 美国在对一些商用低轨卫星的测控中, 采用了商用静止轨道卫星完成与 TDRSS 类似的测控任务, 如采用 INMARSAT 和 ARGOS 卫星来完成跟踪、遥控和遥测。

采用商业卫星完成测控任务, 可以在一定程度上缓解测控资源紧张的矛盾。我们国家的测控系统也可以借鉴此思路, 在通信卫星系统设计时就考虑整个测控的需求, 可以充分利用已有的在轨卫星资源满足不断增长的航天测控需求。

### 3 国内航天测控现状

在国内, 航天测控也已经历了从分离测控体制到统一载波测控体制的过程。目前已建成两大统一载波体制航天测控网, 即基于 S 频段统一载波测控体制 USB (Unified S Band) 的测控网和基于 C 频段统一载波测控体制 UCB (Unified C Band) 的测控网, 绝大多数航天器的测控都由 USB 和 UCB 测控网完成。

随着技术的发展, 统一载波扩频测控体制以其诸多的优点也逐步进入工程实施阶段。扩频测控体制包括相干扩频测控体制和非相干扩频测控体制, 相干扩频测控体制在少数几颗卫星上开始应用, 而非相干扩频测控体制又因其天然的具备多站多星测控能力更加受到青睐。

我校的全军卫星重点实验室与航天部门合作, 已成功研发出应用于某型卫星的国内第一台非相干扩频应答机, 经过测试, 各项性能均达到或超过技术指标要求。该星将于明年发射, 非相干扩频测控体制的首次应用将为我国航天测控体制的发展迈出坚实的一步。

国内有些研究机构, 也开展了测控于通信融合的新卫星平台研发。总的来说, 还处于实验室阶

段,离工程实施还有不少的路要走。

综观国内航天测控的现状,与国外航天测控水平相比,还存在以下几个方面的差距。

1) 测控站数目少,不联网,无法满足日益增长的测控需求;

2) 天上应答机受器件水平制约,发展较慢。

主要体现在:

- 先进的信号处理技术不能应用,导致测量精度低、抗干扰能力差;
- 测控频段仍停留在原有的 S、C 波段,向更高频段发展困难重重;
- 星载多波束天线技术虽然取得进步,但差距仍比较明显。

3) 中继星仍在建设中,测控覆盖率仍严重受限。

## 4 发展对策

航天测控也是一个系统工程。国内航天测控的发展,有些是受国情因素制约的,需要国家政策扶持,长期才能见到效果,比如航天器件产业。

针对目前的国内外技术层面的差距,认为可以努力的方面如下。

1) 加大预先研究力度,争取在光信号处理、K 频段射频、多波束天线等方面多做技术储备,在技术上缩小与国外的差距,在器件水平成熟时再搬到天上;

2) 军用卫星测控应重点向抗干扰、抗截获方面发展,保障我军用卫星在复杂电磁环境下的生存能力;

3) 研究测控与通信相结合的测控技术体制,在信息速率、测控精度、实现复杂度等方面折衷考虑,实现测控与通信的融合,减小飞行器的体积、重量,充分发挥飞行器有限的资源。

## 5 结束语

夺取制天权的是新军事变革的重要内容之一,航天测控则是保证夺取制天权的基础。根据我国的国情,大力开展我校航天测控学科建设与科研开发,是历史赋予的机遇也是我校义不容辞的责任。

## 参考文献

- [1] 姜昌,范晓玲.航天通信跟踪技术导论 [M].北京:北京工业大学出版社,2003.
- [2] 林墨.深空测控通信发展趋势分析 [J].飞行器测控学报,2005(6).
- [3] 刘嘉兴.深空测控通信的特点和主要技术问题 [J].飞行器测控学报,2005(12).

## 作者联系方式

通信地址:南京市御道街标营2号通信工程学院五队

邮政编码:210007

联系电话:025-80828481

# 军事信息系统装备项目审核管理与评估方法研究

凌孝明 赵纳新 李玉平

**摘 要:** 本文主要结合信息系统装备项目审核管理工作开展的需要,对信息系统装备项目审核管理与评估工作开展的现状进行分析,对相关的概念和工作开展的程序进行了描述,并就如何做好信息系统装备项目审核管理与评估工作,谈了几点粗浅的意见。

**主题词:** 军事信息; 系统装备; 审核管理; 评估方法

## 1 概述

### 1.1 信息系统装备项目技术体制

信息系统装备技术体制是军队主管部门对一定时期内信息系统装备在技术、“三互”能力方面必须遵循的标准、规范和要求的规定,是产品研制、生产、检验验收和工程建设必须遵循的一种共同技术标准,是信息系统装备项目研发、采办、定型,以及全寿命管理的基本依据。

### 1.2 信息系统装备项目技术体制审核管理

信息系统装备项目技术体制审核管理是指在信息系统装备项目立项、研制和定型、装备改造、改进的全过程中对信息系统装备的技术体制的执行情况进行审查、检验和验证,以及信息系统装备技术体制规范审核等工作。

### 1.3 信息系统装备项目技术体制审核管理与评估的目的

为加强信息系统装备技术体制管理,统一全军信息系统装备技术体制,规范信息系统装备技术体制审核工作,提高全军信息系统装备标准化水平,确保作战指挥信息系统实现互连互通,依据中国人民解放军装备建设的有关条例条令和全军信息系统装备相关的技术体制管理规定,对全军信息系统装备研制项目进行审核管理和评估,以保证信息系统装备技术体制在系统研制的全过程中保持一致性。

### 1.4 信息系统装备项目审核管理与评估的基本原则

信息系统装备技术体制审核工作是全军信息系统装备技术体制管理工作的重要组成部分,在审核工作的指导上必须遵循和坚持全军武器装备研发管理规定的基本原则;以通用装备为主不断完善发展原则;统一规划统一管理资源的原则;归口审核避免重复建设的原则;集中统一管理主动协助的原则。其具体在审核管理工作中必须遵循:一是实事求是、严格把关、保证质量和讲求实效,做到公平、公正、公开,自觉维护审核工作的严肃性和科学性;二是以通用化、系列化、模块化为基本要求,坚持走以通用装备为主,走基本型派生的道路,形成全军统一的信息系统装备技术体制;三是以军事需求为牵引,以科技进步为推动,严格按照必要性、先进性、科学性、可行性等方面的要求严格把关,避免重复建设;四是严格遵守全系统、全寿命管理的要求,把好信息系统装备技术体制审核管理的各个环节,确保技术体制在研发过程中的一致性。

## 2 信息系统装备项目审核管理与评估的现状

### 2.1 缺少一体化建设指导

要抓好信息系统装备体制的一体化的建设与管理,必须要建立一体化的建设指导。近年来,在信息系统装备体制建设管理上,虽建立了相应管理机

构,但由于在各个管理的层面,以及在管理与交流机制上的不完善等因素的影响,没有真正形成对全军信息系统装备项目一体化的建设与指导机制。

## 2.2 缺少科学的管理法规

要切实的抓好信息系统装备的体制管理,不仅要建立完善的管理机构和与其相适应的管理机制,更重要的是要建立健全与管理相适应的管理法规,使各项管理工作的开展有法可依。在近年来的管理中,各级虽做出了极大的努力,但终因该项工作涉及面广、影响范围大,在成果综合确认上很难形成统一的认识,从而严重影响了研究成果的转化。

## 2.3 缺少科学的管理手段

现代的信息系统装备项目管理和评估工作,不仅需要管理协调机构和管理法规来支持,更需要先进的管理验证技术手段来支撑。但在目前,还只能是停留在理论到理论、专家到专家,人为的因素多,缺少科学的技术手段来验证传统的经验。

## 2.4 缺少科学的管理机制

为加强信息系统装备项目的建设管理,在一些层面是可以成立领导小组、成立专家组,安排研究管理工作计划。但由于在项目计划、任务下达、队伍组织、与科研衔接、项目验收等方面的管理上存在着不科学、不完善的问题,尤其是一致性的技术体制审核问题,虽有组织却很难发挥效益,使项目的研制很难取得预想的成果。

## 2.5 缺少适应研究的队伍

在信息系统装备项目管理人才队伍建设上,各级领导机关都非常重视。但专家人员结构上存在很多问题,即人为因素多,没有明确的选拔标准;老中青结合研究不够;领导干部多、且深入科研不够;掌握教学和基础研究人才多,了解军事应用少;队伍分散、松散式管理,缺少相应的管理控制机制来约束,从而使研究成果质量、研究成果的实用性、可操作性,与科研的结合性上深受置疑。

## 3 信息系统装备研制项目审核管理与评估方法

### 3.1 建立信息系统装备项目审核管理组织

为做好信息系统装备项目审核管理工作,不仅要加强对信息系统装备项目审核管理与评估方法,以及相关的理论研究,更重要的是要建立和完善信息系统装备项目审核管理的组织机构。通常应建立信息系统装备项目审核管理领导小组,信息系统装备项目审核管理办公室,信息系统装备项目审核管理专家委员会,信息系统装备项目审核管理专业审查组,以及与信息系统装备项目审核管理专业审查组相配套的初审专业组。

### 3.2 明确信息系统装备项目审核管理工作的程序

信息系统装备项目审核管理工作程序,主要由报审、初审、会审、审批、检查和符合性验证等阶段活动所组成。

#### 3.2.1 报审阶段

各军兵种信息装备部、以及分管信息装备的部门,应根据信息系统装备项目审核的要求填写报审表,向信息系统装备审核管理办公室提交审核申请,并报送以下材料:一是信息系统装备技术体制审核报审函;二是填写全军信息系统装备技术体制审核申请表;三是待审核的信息系统装备技术体制相关文件;四是提交新遵循的信息系统装备技术体制和标准规范审核要求,所拟制的相关的文件资料。

#### 3.2.2 初审阶段

信息系统装备项目审核管理办公室依托相关业务部门,根据报审单位上报的申请表和待审核的相关文件内容,组织相关的专家对报审材料进行初审,并提出初审处理意见。初审的主要工作:一是报审项目是否列入年度审核计划;二是报审项目的时机是否成熟;三是送审的信息系统装备技术体制文件格式是否符合要求;四是报审文件是否齐套;五是材料中有关信息系统装备技术体制的内容描述是否清晰、明确和完整;六是报审材料内容是否符合全军信息系统装备技术体制发展的要求,提出初



审意见；七是对审核中出现不符合要求的报审文件时，应及时的上报管理办公室，并提出退回和重报的意见。

### 3.2.3 会审阶段

信息系统装备项目会审是在完成初审的基础上，依据初审过程中遇到的异议问题，确定会审专家名单（有关业务部门下设的初审专家库），组织会审专家对报审材料进行会审（在特殊情况下也可以函审的方式），形成会审意见；此外，还应根据提出问题的重要程度，向上一级专家委、专业审查组提交，并提出审核意见，再报管理部门。其会审前的主要工作：依据初审过程中遇到的疑难问题，确定会审专家名单，并完成以下准备：一是制定会审计划、确定会审日期、会审地点、明确审核专家组组长、成员名单；二是参加会审的专家要了解受审单位的基本情况，查阅受审单位的相关文件。组织会审的基本程序：一是管理办公室介绍受审项目的背景和基本情况；二是简要介绍实施审核采用的方法和程序；三是提供会审专家组与受审单位之间联系方式；四是介绍和说明审核过程中不明确的内容；五是根据审核工作需要，对担任会审的专家提出进一步的审核要求和保密要求；六是对审核中遇到有异议的问题，管理办公室负责协调受审单位向审核专家组进行解释、说明和沟通，形成一致审核意见后上报管理办公室。

### 3.2.4 审批阶段

信息系统装备项目的审批，是在审核专家组通过会审形成的审核意见的基础上，报信息系统装备项目管理办公室进行审批，并回复报审单位。对于通过审核的项目，报审单位将审核意见随有关文件，一并上报总装备部；对于未通过审核的项目，报审单位应根据专家意见重新论证并对编写有关文件进行修订，再申请上报。在重新审核中，如仍然存在严重问题，将终止该项目的立项审核。各单位上报的受审文件经办公室审核通过后，统一发布实施。列入国家军用标准计划的，按国家军用标准管理办法实施。

### 3.2.5 检查

对信息系统装备项目检查，是落实信息系统装备“系统”、“全寿命”管理的一种方法和措施，通常是在信息系统装备项目过程中组织，由信息系统

装备项目审核管理部门组织，主要检查项目执行单位落实和执行评审意见情况。

### 3.2.6 符合性验证

信息系统装备项目符合性验证，主要是指对信息系统装备技术体制的符合性验证，是在全军通定委定型试验时组织验证；专用装备在定型之前进行技术体制验证试验，可由信息系统装备项目管理办公室或定型办组织，在信息系统装备试验基地或在指定的单位地点实施。

## 3.3 确立信息系统装备项目审核管理及评估的内容

信息系统装备项目的审核内容，应根据全军相关的信息系统装备管理规定来确定，通常包括：各单位上报的受审文件中，信息系统装备技术体制、信息装备技术体制规范等方面的符合性问题。其主要审核内容包括：一是单独安排研制和纳入武器系统安排研制的配套的信息系统装备的立项综合论证报告、研制总要求（技术体制与立项方案发生变化的）、定型前的技术体制符合性检测和定型、鉴定文件；二是选购民用信息设备、引进信息装备，以及随武器系统配套引进的信息装备的战术技术指标和产品技术规范；三是军内装备科研计划、装备技术革新计划及自筹经费安排研制的信息装备的战术技术指标、研制方案；四是信息系统装备技术体制标准规范论证报告；五是在信息系统装备研制全过程中，有计划的组织对技术体制的审核意见执行情况进行检查。

## 3.4 科学的运用信息系统装备项目验证和评估的方法

依据信息系统装备“全系统”、“全寿命”管理的要求，在信息系统装备项目研制过程中，应对技术体制审核意见执行情况进行检查和符合性验证及评估。由信息系统装备项目审核专家组，对待检查信息系统装备项目的技术体制符合性测试大纲、测试方法、验证和评估方法、指标体系等要素进行评审把关，并指定相关单位按照检查项目的标准要求，逐条进行测试取证、检查验证和评估，并详细的记录不符合项的内容和问题。信息系统装备项目审核专家组根据符合验证评估的情况，向信息系统装备项目管理办公室提交综合性评价意见。符合性

验证评估的结论分为三种形式：即“审核通过”、“存有异议推迟通过”、“审核未通过”。通常对审核为“通过”的项目，由审核专家组将审核评估报告上报管理办公室备案；对审核为“推迟通过”的项目，由被审核单位依据提出的修改意见，以及与审核专家组商定的期限（至少两个月）完成修订稿，并达到规定的要求，书面报告上报管理办公室。管理办公室再组织审核专家审核提交的整改报告，并可到装备研制现场进行复核；对审核为“不通过”的项目，被审核单位依据提出的修改意见，尽快地制定整改措施，并在6个月内完成整改，可重新向管理办公室提出复审申请。对复审后仍“不合格”的项目，应退回受审单位不再行申报。

## 4 加强信息系统装备研制项目审核管理与评估系统建设的几点建议

### 4.1 突出一体化的规划管理

从未来联合作战指挥的整体性角度考虑，所研制信息系统必须要能与其他子系统彼此相联、相互融合，最终将各子系统发展成为一体化作战体系中的有机的的重要组成部分，并与作战体系整体功能紧密结合发生本质的改变。因此，现在信息系统装备项目论证、规划必须严格贯彻一体化设计理念。

### 4.2 必须规范项目论证管理

为尽快理顺全军信息系统装备项目论证管理的秩序，必须加快对信息系统装备项目审核管理工作相关的管理规范、管理规定等研究成果向法规转化的进程。同时，要强化对执行法规的行为进行规范，尽快地理清全军信息系统装备体制管理的工作

参考文献（略）

作者联系方式

通信地址：北京市丰台区大成路13号Z02

邮政编码：100039

联系电话：010-66820167

思路，尽快的理顺全军信息系统装备体制管理审核秩序。

### 4.3 必须强化统一管理控制

在建立统一规划管理的基础上，还需加强统一的建设管理与控制，不仅要加强统一的建设规划、建设方案技术体制的审核，而且还必须遵循“全系统”、“全寿命”的原则，在项目建设研究的全过程中进行跟踪把关，使有限的信息系统项目研制经费用到实处，使统一的建设需求、建设思路和顶层的总体设计落到实处，尽快的解决未来信息化战争中作战指挥信息系统的“三互”问题，尽快地实现战略、战役、战术层次的一体化指挥。

### 4.4 必须加大验证研究投入

为使信息系统装备项目论证、研制工作更加贴近实际，使审核管理工作更加准确和严谨，使管理手段更加科学有效，在强化一体化设计、加大规范化管理的基础上，还必须根据信息系统装备技术发展和管理工作的需要，加大信息系统装备体制管理审核验证手段建设和研究的投入，以解决当前信息系统装备项目审核管理的急需。

### 4.5 必须建立科学的审核管理计划机制

信息系统装备项目管理研究不仅要有领导重视、需要加大研究的投入、需要建立审核机构、需要人才队伍的建设，但更重要的是要将其真正的纳入科研的整体规划，建立起经常性的审核管理计划、建立起经常性的审核管理协调机制，以增强信息系统装备项目管理的科学性，减少信息系统装备项目管理工作中的盲目性。

# 美军运用民用信息技术 打造军事信息系统理念对我军影响浅析

王刚 鲁岩 程磊

**摘要：**本文从我军新世纪军事信息系统的发展出发，介绍美军提出的全球移动信息系统（GLOMO），同时探讨研制合成电子战系统提高我军信息化水平的可行性，并重点研究运用成熟的民用信息技术打造我军军事信息系统的指导思想和原则，以及在实际运用过程中应当着重解决的问题。

**关键词：**民用技术；信息技术；信息系统

## 1 新世纪我军军事信息系统概况

由于电子信息技术迅猛发展，新的世纪是信息的时代，人类将进入信息社会。不言而喻，信息时代的战争必将是信息化的战争。美国前国防部长拉姆斯菲尔德明确提出：21 世纪的战争形势为核威慑下的信息化战争。因此，在 21 世纪进行作战的部队必须是信息化的部队。当今电子信息技术的发展在很大程度上是基于电子信息技术的数字化，信息化部队也可以称之为数字化部队，信息化战争的战场也可称之为数字化战场。而其实质含义是：数字化部队是以数字通信为基础，使部队的指挥控制、情报侦察、预警探测、信息利用和信息对抗一体化，武器装备智能化；数字化战场就是利用现代数字化通信手段和计算技术把战场上的武器系统和战斗部队连接成一个整体。军事信息系统是指在作战中所使用的信息系统，主要包括人员、机器、手工和自动程序，以及能够收集、处理、分发和显示信息的系统，如：一体化的指挥、控制、通信、情报、侦察与监视系统（IC<sup>4</sup>ISR），以及指战员信息网（WIN）等。

计划，以满足国防上对快速展开和可靠的信息系统的需求，并研究和验证支持这一需求的各项技术。推动（GLOMO）计划的一个实例就是陆军推出的数字化战场，而其主要是将无线局域网、战斗网无线电台（CNR）、地面个人通信系统（PCS）、基于卫星的个人通信系统、直接视频广播等通过单信道无线电入口（SCRA）和无线入口点（RAP）接入大容量干线网电台无线网（HCTR），从而构成栅格状战区通信网。同时，（GLOMO）计划的提出一方面是要满足未来国防上有效的移动信息系统的需求，而另一方面又能利用发展中的民用信息技术，当然，军用信息技术的技术要求与民用信息技术的要求相比，有许多特殊要求：军用上需要有快速展开的基础设施，而只有有限的入口；网络拓扑应高度动态，用多跳分散连接；数据流和指挥与控制采用动态分配和优先制；在敌对环境中信息率要达到最大；保证系统和信息的安全；具有顽存性的高度动态的高级服务等。而其中军事信息系统应具有在复杂战场环境中的适应性是一个重要的技术要求，如在移动性低的环境用宽的带宽，而在移动性高的环境，则用窄的带宽。系统要能快速展开，具有高度机动性。此外，军事信息系统在安全性方面还要求具有抗多径干扰、敌方干扰、环境噪声干扰和具有多级保密等技术要求。全球移动信息系统（GLOMO）由 4 个系统层组成：最低层是基本的低功率、高能力、能在运动中工作的硬件和固件，即提供一种具有足够处理能力的无线电台，以支持移动组网；第二层为不限定的节点与组网技术结合起来提供可靠的无线通信网络；第三层为由无线和固定两种网络组成的端到端的网络；最后一层为充

## 2 全球移动信息系统（GLOMO）概述及其主要结构

### 2.1 全球移动信息系统的性能要求

20 世纪 90 年代中期，美国防高级研究计划局（DARPA）提出了全球移动信息系统（GLOMO）

分利用移动通信能力和移动计算以适应变化的分散的连接。

## 2.2 全球移动信息系统的主要结构

全球移动信息系统主要由系统工作的工具、语言和环境设计的基础设施；高性能、模块化、低费用和小功率的不限定无线节点；移动组网算法和协议、自组织、自愈技术、可靠的算法和快速展开的无线网络；在异种混合网上工作的端到端组网等主要部分构成。

美军全球移动信息系统的一个重要设计思路是使该计划的成果综合进民用产品，从而使下一代军事系统能以商用产品和业务为基础，而其主要目标是要为全球移动环境中可靠的端到端信息系统开发技术，为把基础的商用元部件综合进灵活、可靠、多跳的宽带系统中去。为此，美国军方充分利用了民用数字信息处理和分支技术、GEO 与 LEO 卫星通信网络综合技术、个人数字助手（PDA）和类似技术保障终端用户的计算机接入技术、多媒体通信的异步传递模式（ATM）等发展成熟的民用信息技术。

## 3 美军合成电子战系统概述及主要特点

在信息化战争条件下，电子对抗（ECM）和电子反对抗（ECCM）这一对矛盾对敌我双方都是生死攸关的问题。通信系统、侦察系统和电子对抗系统任何一方都是必不可少的。它们之间既有相互矛盾、相互制约的一面，同时又有相辅相成的一面。长期以来，这两个领域的发展与研制都是独立进行的。但在实际运用当中，由于各种原因，它们之间会产生矛盾与冲突，如果不很好地协调处理，将会导致相互影响而不能发挥应有的作用。甚至会造成不良的后果。

### 3.1 合成电子战系统概述

合成电子战系统，即具有自行组织、自行管理、自行运行、自行适应功能的，综合完成通信、侦察、电子对抗任务的一体化的系统。在世界范围内不仅已经有了先进的通信系统、侦察系统和电子对抗系统，且其自动化、智能化的水平也在不断提高，如各种类型的 C<sup>4</sup>ISR 系统、智能网络、自组织

信包无线通信网、ISDN、神经元网络等新技术的发展已为构成合成电子战系统提供了技术基础。

## 3.2 合成电子战系统基本性能特点

合成电子战系统其结构的主体部分为通信、侦察、电子对抗等子系统，但它们是一个有机的整体。对客观情况变化时的探测和判断由支援子系统完成。控制子系统则完成自组织、自适应的功能。点对点的通信已经满足不了现代化战争的要求。单个合成电子战系统是远远不够的。实际上必须把许多合成电子战系统连接成网，它相当于把地域通信网中各个结点换成合成电子战系统。合成电子战网不仅各个系统具有自组织自适应的功能，整个合成电子战网还应具有网络功能，即能自行组网、自适应结点的被摧毁和链路的中断及恢复等网络的自组织、自适应功能。把系统和网络的功能结合起来，将更加发挥其威力。合成电子战系统除了通信、侦察和电子对抗外，其进一步的发展为与武器系统的指挥和控制结合起来，形成通信、指挥、控制、对抗、情报系统。

## 4 对我军建设军事信息系统的启示

美军在研制和发展全球移动信息系统（GLOMO）和合成电子战系统的过程中，特别是在建设 21 世纪数字化战场通信中都强调了军用技术和民用技术、军用产品和民用产品的结合，以及军民两用相互促进的思想和原则，并取得了显著的效果，对提高美军的信息化技术和信息化作战水平，促进美军的军事转型都有重要的意义。美军的成功经验，对于我军发展军事信息系统有着重要的借鉴意义。

### 4.1 充分利用成熟民用通信技术和基础设施

美陆军在建设军用信息系统时，在其基础技术方面利用了新颖的商用通信资源，以增加现有的战术通信系统的能力。近年来，随着我国移动通信和卫星通信技术的飞速发展，我军研制军用信息系统时可以而且也应该从这些新的通信技术中受益，如充分利用民用的通信基础设施，提高军用通信的质量，以避免浪费。另外，我军传统军事专用通信设备数量较少，一直是小批量生产，所以不能满足危

机时刻迅速齐装,这种状况进一步促使我军采用民用现成设备,以便在短时间内利用民用制造商的基础设施,从而获得大量的设备,以满足部队迅速部署的需利用我国民用制造的基础设施来满足部队快速部署的需求。同时,作为我军建设军用信息系统计划的一部分,民用技术可用在训练与条令司令部的用户环境中,如我军可以利用共享的 ISDN 商用现成的硬件和软件技术,并与全球商用基础设施相连接。

## 4.2 充分利用民用卫星通信和ATM交换技术

在未来战场上个人通信业务(PCS)和数字蜂窝技术将在新的战场信息传输系统(BITS)中发挥重要作用。而 LEO/GEO 卫星或无人空中飞行器不需要复杂的地面基础设施,在许多应用方面更富吸引力,其将成为未来战场通信的一个重要组成部分。我军应当在未来 10 年将着重采用民用技术,以便能够减少设备与寿命周期费用,同时改善系统性能和经济上的可负担性。研究由军民两用技术组成的综合体系结构,在保证战场双重基地作战的各个阶段能确保通信系统的可用性。与此同时,ATM 交换技术已成为下一代战术交换技术。将推广研究在战术互连网采用商用标准 TCP/IP 协议的分组交换系统。美国陆军正是充分的利用了该项技术使得其现有的数据网(MSE、EPLRS 和 SINGARS)将采用基于商用互连协议的战术多网关(TMG)和网间控制器(INC),实现无缝隙互连。

## 4.3 以核心计划发展为牵引,促进民用技术向军用技术的转化

美军在发展全球移动信息系统(GLOMO)时,计划把全球移动信息系统所开发的技术作为新的民用无线信息系统和业务的催化剂,通过民用产

品和业务使这些技术可供军用。特别是美国国防部选定基础和应用的开发与开发项目,它从事的研究和技术开发风险和收效都很高,而且,如果成功的话,可以大大促进传统的军事任务和使命以及军民双重应用。为此,美军军方提出全球移动信息系统(GLOMO)计划是由于要满足将来国防上对有效移动信息系统的需求,而同时又能利用商业部门发展中的技术,其一个重要思路是使该计划的成果能综合进民用产品,从而使下一代军事系统能以民用产品和民用业务为基础。而其最终的目标是要为全球移动环境中可靠的端到端信息系统开发技术,为把基础的民用元部件综合进灵活、可靠、多跳的宽带系统开发技术中去,而在“端到端”组网中使用和扩展各种可用的商用标准,以使移动环境真正是全球信息基础设施的一部分。将开发使无线网络与 NII 相结合的技术,因而有机会利用任何可用的通信设备,例如蜂窝系统、个人通信系统或卫星通信接入 INTERNET。因此,我军在发展军用信息系统的过程中,可以充分的发挥军事需求的牵引作用,开发出性能稳定、运转高效的民用信息系统,使军用技术和民用技术得到充分的结合,最后促进军用技术与军用技术的整体提升。

充分利用已有的民用系统,在最短的时间内,弥补军用系统之不足,完成整个军用系统的布置,是我军信息化建设特别是建设军用信息系统的一个重要的途径。总之,充分利用民用信息技术,建设我军军事信息系统是一种具有战略性的指导思想和原则,在国防现代化建设中应以应用和贯彻。同时,随着商品经济的发展,今后在军民两方面,在诸如管理体制、经费使用、人力资源、流通渠道等等都要相应的政策,才能为军用和民用相结合创造必要的条件。

## 参考文献

- [1] 李承恕.《自组织自适应综合通信侦察电子对抗系统无线电工程》.1991年12月
- [2] B M Leiner, et al. Goals and Challenges of the DARPA GloMo Program. IEEE Personal Communications, Dec 1996: 34~43
- [3] 《21世纪数字化战场通信》(译自 IEEE Communication Magazine)

## 作者联系方式

通信地址:海南海口市海秀大道海南省军区装备部

邮政编码:570236

联系电话:0898-66571655 13876765315

# 用创新机制提升中国软件产业自主创新能力

吕品 吕家国

**摘 要:** 提升中国软件产业自主创新能力是促进中国软件产业快速发展、提高国际竞争力的必由之路。建立适应中国软件产业发展要求的外部环境条件,促进自主创新能力的迅速提升,是推进中国软件产业发展的关键所在。本文在分析研究制约中国软件产业自主创新能力提升瓶颈的基础上,从改革和创新机制角度讨论了如何提高中国软件产业的自主创新能力。

**关键词:** 软件产业; 自主创新; 完善机制

进入 21 世纪,软件产业已经成为推动经济发展、促进社会进步和保障国家安全的重要因素。软件技术成为信息技术的核心和灵魂,成为快速发展的一个新的技术领域和新世纪国际高技术竞争的一个重要制高点。在信息技术竞争越来越激烈的今天,一个国家软件产业的兴衰成败,将在很大程度上决定她在国际竞争中的地位。为适应全球信息技术快速发展的要求,中国已经把软件产业作为优先发展的战略性新兴产业。中国软件产业实现发展与壮大,走向世界,不能简单地仿效国外软件产业的发展方法,重复外国软件产业的发展道路,要在充分考虑世情、国情和行情的基础上,遵循产业特点及发展规律,制定符合我国软件产业的发展战略和规划,推进中国软件产业创新发展特别是自主创新发展。本文在分析中国软件产业自主创新存在问题的基础上,着重讨论通过创新机制提升中国软件产业的自主创新能力。

## 1 制约中国软件产业自主创新能力提升的瓶颈

总体上看,目前中国软件产业处在一个向前发展的机遇期。相对于蓬勃发展的国际软件业,中国软件产业发展仍处于“初级阶段”,存在着规模小、国际市场占有率低、创新发展能力弱等方面的问题。中国软件产业创新发展的瓶颈在机制滞后,出路在创新机制。从产业体制看,存在着从研发到产品的“两张皮”的现象,即从前期研发创新到后期产业化过程(生产、市场、推广、服务、升级等),各环节缺乏良好的衔接,自主创新的基础弱化;从创新主体看,企业过多强调自主创新存在的

风险因素,不愿增加或不愿向自主创新进行投资,自主创新发展的后劲不足;从创新环境来看,针对软件产业这一特殊领域的法律、法规和手段还不够健全,软件产业创新成果的保护力度不够,自主创新外部环境较差,等等。

### 1.1 研发投入不足,缺乏自主创新发展的后劲

为保持企业持续不断的竞争能力,国外大型软件企业非常重视自主创新,不断增加研发投入。2005 年,微软公司研发投入高达 465.9 亿美元、BMC 软件公司高达 58.6 亿美元,而目前中国软件企业乃至整个 IT 产业由于受创新研发周期长、投资风险大等因素的影响,在研发领域普遍存在投资不足,水平偏低等现象。2004 年研发投入超过 10 亿元人民币的 IT 类企业仅有华为、中兴、海尔、联想等 6 家,而信息产业部评选的“中国电子信息百强企业”的研发投入总额仅为 266 亿元人民币,比思科公司 2003 年度的研发投入略多一点。截至 2003 年底,中国软件业各类从业人员大约有 620 万人,从事研发人员总数仅为 11.9 万人。财力和智力投入不足严重制约了中国软件产业自主创新能力的提高和国际化进程的发展。

### 1.2 产业链条脱节,自主创新发展的基础薄弱

中国大多数软件企业受规模及研发实力的限制,长期从事的仅是代码实现的工作,主要产品依附于国外的软件平台,缺少自主产品设计,直接影响了企业创新能力的提升,导致自主创新能力的基

础比较薄弱。许多企业缺乏长期发展思路,忽视自主创新的基础建设,把自主创新简单地理解为是科研机构的事,多着眼于使用现成的技术带来短期经济效益。而高校、研究所等研究机构的创新成果由于得不到企业的重视和使用导致了创新成果转化率低,经济效益不明显,影响了创新研究的积极性。研究机构和软件企业在创新环节上的脱节也导致了创新研究成果不能很好的适应市场需要,陷入了科研与生产脱节的恶性循环之中。

### 1.3 产权保护不力,影响了自主创新发展的积极性

计算机软件作为一种特殊的社会产品,具有易复制、易传播且边际成本极低等特点,导致软件盗版行为屡禁不止,软件盗版现象猖獗。随着计算机技术的迅速发展与普及应用,社会对软件产品的需求增长加快,同时盗版技术和手段也越来越成熟,一个投巨资研发的产品,一旦推向市场,很快就被盗版。据美国商业软件联盟调查数据,2004年中国市场软件使用盗版率超过90%。除知识产权保护观念淡薄这个根本原因外,软件产品知识产权保护立法滞后,法律缺陷、执法不严和执法手段落后已经极大地制约了软件产业自主创新发展,并严重挫伤了软件企业自主创新的积极性。

## 2 用机制创新推进中国软件产业自主创新发展

对高科技产业而言,特别是对于像软件产业这种在中国正处于起步阶段的产业来说,改革和创新中国软件产业快速发展的运行与保障机制,为其提供一个良好的外部环境,必将对产业的发展 and 自主创新能力的提高起到巨大的指引、规范和推动作用。

### 2.1 完善运行机制 建立科学、高效、规范的中国软件产业链

中国是软件需求的大国,同时也是软件生产的小国,软件产业与中国的经济结构和国际地位极不适应,影响了中国的经济发展和在国际上的大国形象。中国软件产业的现状是企业规模小、从业人员少、创新能力弱,缺乏主导产品,科研、生产、销

售、服务、升级一体化程度低,无法形成强大的国际竞争实力。只有打破目前这种分散经营、各自为政、“小打小闹”的现状,通过整合各种、各类资源,构建强大的中国软件产业链条,才能真正提升国际竞争能力。实现上述目标,必须从如下方面入手:成立有权威、有权力的领导管理机构,加强对中国软件产业的创新发展进行有效管控;加大对软件产业的投入,完善有利于产业发展的投、融资政策,切实解决软件企业在创新研发资金方面所存在的筹资和融资困难等问题。对有自主研发能力的企业,要从政策、资金等方面给予扶助;从国家战略高度支持重大基础软件项目的研发与创新,政府要在软件产业风险投资方面承担更多的责任,特别是在自主创新发展过程中的风险投资承担更大的义务;政府要采取措施鼓励中国软件企业研发自主产品,为软件企业与科研院所和高等院校之间的技术合作搭建桥梁,从而形成高校与科研院所、软件企业之间在人才、技术与资金方面的密切合作、良性互动。加强企业与高校和职业培训机构在软件人才培养方面的合作,加快培养高智力的创新人才,成为产业自主创新的带头人。加大高等教育改革的力度,注重“教育为产业发展服务”的实效性,通过各种途径,大力培养基本功扎实的开发型人才,成为产业自主创新的骨干。综合多方面的因素,真正形成一个有实力、有活力、有竞争力的软件产业链。

### 2.2 建立合作机制,促进软件企业联盟的形成

针对中国软件产业的总体规模还比较小、市场占有率低以及国际竞争力较弱等问题,要在鼓励和确保大企业和骨干企业发展的同时,鼓励软件大企业与小企业之间进行合作,促进软件企业联盟的形成。加强软件企业之间市场信息和研发、管理经验的交流,形成优势互补,共同应对创新风险;企业要结合自身优势及特点加强与其他企业之间的联合,共同承担软件基础研发任务;在产品合作开发以及销售等方面合作,共同参与国际市场的竞争;发挥本国软件企业对国内市场熟悉程度高,变化反映快的优势,不断推出创新型产品,扩大在国内软件市场的占有率,逐步提升中国软件产业的整体竞争力。从另一个角度看,中国软件产业实力越强,发展越迅速,主导产品越多,国际市场占有率越

高,也能够从根本上改变中国在软件领域的不良形象。

### 2.3 强化保护机制 营造良好的自主创新发展的外部环境

软件产业是一个特殊的领域,软件是一种特殊的社会商品,软件保护具有很强的特殊性。中国软件产业创新发展春天的到来,需要一个适合的外部环境,其中软件保护是实现该任务目标的当务之急,重点做好以下方面的工作。

1) 广泛宣传知识产权保护的重要性,提高全社会知识产权保护意识。要加强全民知识产权知识的普及与教育,转变长期以来形成的“盗书不为窃”的传统观念,改变“知识无国界”的片面认识,自觉参与软件知识产权的保护。

2) 加强软件知识产权保护技术的研究,增强软件自身的保护能力。采用构件技术对软件产品进行封装,使软件像硬件一样成为有形的商品;采用特殊的加密技术对软件产品进行包装,增大软件产品的盗版难度。

3) 从立法和执法两个方面加强知识产权保护,加大打击软件盗版行为。完善现有的法律法规,用法律手段规范软件市场行为,特别要注重用

经济手段对软件盗版的非法行为进行严惩,增大软件产品盗版的成本。

4) 建立完善的软件产业服务保障体系,使盗版软件因无法得到后续支持而失去价值。

## 3 结束语

在新一轮高新技术产业化发展和高新区建设中,从国家到地方已经将软件产业作为提升核心竞争能力的重要途径从战略高度加以扶持,各种促进提升中国软件产业自主创新能力的配套科技政策已经或正在酝酿出台,软件产业已成为许多高新区重要的经济增长点。一个成熟、稳定、有效的运行和保障机制必将规范和促进中国软件产业自主创新能力的提升和行业的快速、健康发展。以自主创新为驱动力的软件产业对高新技术产业化发展起着巨大的带动作用,也必将对中国经济的可持续发展,对建设创新型国家发挥更大的作用。从另一个角度看,中国软件产业实力越强,发展越迅速,主导产品越多,国际市场占有率越高,也能够从根本上改变中国在软件领域的不良形象。

### 参考文献

- [1] 曹方. 创建产业生态系统,增强软件产业自主创新能力[J]. 软件世界, 2006,(5): 67-70.
- [2] 刘文彬. 发挥政府在软件产业发展中的促进作用[J]. 大连干部学刊, 2006,22 (6):36-37.
- [3] 刘子军. 浅论中国目前软件产业科技发展创新与对策[J]. 科学咨询, 2004,(4):21-23.
- [4] 陈存友, 王成. 中国软件产业发展初探[J]. 软科学, 2003,17(2):38-41.
- [5] 曹巍, 王元地, 孟齐美. 中国软件产业发展的现状分析与发展建议[J]. 科技管理研究, 2006,26(8):32-34.
- [6] 孟微, 钱省三. 印度软件产业研究[J]. 科研管理, 2005 (1):113-117.

### 作者联系方式

通信地址: 中国科学院软件研究所综合信息系统技术国家重点实验室

邮政编码: 100080

联系电话: 13811711698



# 俄军对信息战的研究与准备

庞海东 白永祥

**摘要：**“信息战”的理论是美国在 80 年代中期提出的。俄军已经把对信息战的研究提到议事日程，并开始组织较大规模的学术研究和探讨。可以说，俄军对信息斗争的重视态度既是受西方“信息战”理论和实践冲击的结果，又是俄军建设自身发展的必然。因此，俄军认为，在进一步实施员额裁减，而担负的保卫国家安全的任务并未减轻的情况下，大力推行信息技术在军事上的应用，并且重视保护信息安全，具有越来越重要的意义。

**关键词：**俄军；信息战；研究；准备

关于信息技术在作战上的应用，早在 20 世纪 80 年代以前苏军就有过研究，并且进行过应用试验。但是，把“信息战”作为一种作战样式加以研究，并且开始认真思考和筹划信息斗争的理论与实践，研究对付信息战的反措施，则是近年来的事。可以说，俄军对信息斗争的重视态度既是受西方“信息战”理论和实践冲击的结果，又是俄军建设自身发展的必然。

## 1 对信息战和信息化部队建设的研究开始起步

“信息战”的理论是美国在 80 年代中期提出的。海湾战争后，美国等西方国家开始对其大肆加以渲染，并着手付诸实践。俄罗斯建军伊始，出于种种原因，对西方的信息战并未引起足够的重视。近一、两年来，俄军受新军事革命浪潮的冲击，越来越强烈地意识到了西方军队信息化建设咄咄逼人的态势，同时也由于军队建设逐步走上正轨，俄军开始重视信息战和信息化部队建设的问题。首先，俄军承认自身在信息斗争领域的研究和实践都已“落后于西方”的事实，认为在今后一个时期内必须加快这一领域研究的步伐。俄军已经把对信息战的研究提到议事日程，并开始组织较大规模的学术研究和探讨。除俄军科研机构和军事院校开展广泛研讨外，俄还开始与国外进行有关学术交流。1995 年，俄、美两国军事专家就“信息战”问题举行了联合专题研讨。同年 11 月，俄联邦安全会议部长委员会根据研究机构的咨询意见，向国家首脑呈交了“关于信息安全”的报告，阐述了信息安全和信

息斗争的意义。

## 2 提出对“信息战”的看法

俄军事理论界在研究了西方特别是美国的“信息战”理论，探讨了近几场局部战争特别是海湾战争的实践，总结了俄罗斯军事技术和战争实践的发展历程和现实状况之后，对信息在军事领域的应用和“信息战”提出了以下看法。

### 2.1 信息已经成为控制世界的决定性因素之一

关于“信息”和“信息战”的作用，俄军事理论界认为，美国提出的信息战理论“不乏故意渲染和夸大的成份”，但从总的发展趋势看，现代社会离不开信息，信息是推动社会变革的力量。伴随着 21 世纪的到来，人们凭借物质对象进行的工作越来越少，更多的将是借助信息进行工作。到 2000 年，发达工业国家将有 60% 的人口凭借信息进行工作。美国等西方国家高度重视信息绝非偶然，因为“信息已成为控制当今世界的决定性因素之一”。“信息是否准确、及时和完整，在很大程度上关系到能否顺利解决政治、经济、国防、科学、教育、文化等一系列问题”。信息和信息技术不仅能用来创造物质财富，而且“已经取代传统的武力手段成为维护国家利益的有效武器”。信息应被看作是“战略资源”，充分利用信息手段，可以大幅度提高军队的战斗力。因此，俄军认为，在进一步实施员额裁减，而担负的保卫国家安全的任务并未减轻

的情况下,大力推行信息技术在军事上的应用,并且重视保护信息安全,具有越来越重要的意义。

## 2.2 信息广泛地应用于军事领域,是必然趋势

俄军认为,将信息手段运用于军事领域,用作相互对抗的一种手段并非新生事物,早在古代就有。冷战时期,两大对立的阵营曾广泛地利用信息手段相互向对方施加政治、精神和心理影响。有的专家甚至认为,华约之所以垮台,苏联之所以解体,“美国和西方的信息攻击起了不可忽视的作用”。随着人类步入“真正的信息社会”,信息必将更广泛地应用于军事领域。

## 2.3 信息战的首要打击目标是指挥控制系统以及民心士气

俄军认为,较之武装斗争的其他手段,信息打击的目标将更广泛,既包括军事目标,也包括非军事目标,以及国家领导与管理系统、经济体系、金融财政系统,甚至普通民众。在军事目标中,首当其冲的是武装力量的指挥控制系统,包括各级各类指挥所、情报中心和控制中心。在民用目标中,最易受攻击的是行政合理系统、银行等主融系统,以及民众的心理。从某种意义上说,对武装力量人员和居民心理等“软”目标实施的信息攻击所产生的效果、可能比对“硬”目标实施信息攻击所产生的效果还大。

## 2.4 信息打击既可以使用普通手段、也可以使用特殊手段

俄军认为,在未来信息战中,将广泛使用各种信息武器。主要包括:广播、电视、报纸等大众新闻媒介,以及派遣人员进行渗透,针对的主要是敌国普通民众和社会;专门的、特殊的信息武器,加计算机病毒、信息炸弹、逻辑炸弹、被赋予了特殊使命的计算机芯片、能产生电磁脉冲的爆破装置、超高频发生器、能对电子仪器和电讯器材起破坏作用的电子生物武器等,其方式是破坏、歪曲、阻塞信息流通,主要目标是敌国军队的指挥控制系统和各类武器系统,国家的通讯系统、银行计算机系统、陆上、海上和空中的交通管制系统,甚至国家选举自动表决系统以及其他与国家安全密切相关的

系统。信息战可以单独实施,也可以同其他类型的作战手段配合实施。

今后一个时期内,敌国可能针对俄罗斯发动的信息战样式。俄军认为,当前以及今后一个较长的时期内,俄罗斯将不大可能面临大规模入侵的威胁,因此抓住时机、“复兴俄罗斯”是俄面临的艰巨任务。力完成这一任务。必须保持“俄罗斯的统一,民族团结和社会和谐”,保持武装力量的战斗力。而敌对国家恰恰可能趁俄罗斯由旧体制向新体制的转轨时期,千方百计破坏俄罗斯的稳定,削弱俄罗斯,“给俄罗斯的复兴造成障碍”。为达到这个目的,发动信息攻击是最佳手段之一。敌国将通过政治、经济、军事和社会生活的各个渠道对俄国家领导决策层、武装力量以及其他专政部门、普通民众实施信息攻击,误导领导人做出于敌有利,于己不利的决策;使俄武装力量斗志涣散,纪律松懈,战斗力下降;使民众的心理受到伤害和扭曲,意志受到动摇,精神和道德陷入沦丧;使民族之间产生更多的矛盾和隔阂,并导致国家分裂,一些俄罗斯专家认为,如今俄罗斯社会出现的一些心理变态、犯罪等消极现象,除了自身原因外,还与西方的信息攻击有直接的关系。在敌国对俄罗斯发动信息战时,将有可能使用特殊信息武器,如可造成人员心理变态和精神失常的武器。另外,作为一种遏制手段,一些西方国家将竭力阻止俄掌握先进的信息技术,把俄排斥在先进的信息网络之外、从而一直保持对俄罗斯的信息技术优势。

## 3 研究和制定反信息战的措施

在美国等西方国家大力推行军队信息化建设的情况下,俄军认为,必须把防止和抗击“信息侵略”提高到保卫俄罗斯国家利益的高度,认为有无抗击信息侵略的能力“决定着国家和武装力量的未来”。因此,必须把研究和制定反信息战的措施作为俄军建设的一项任务,尽早提到议事日程。有的学者提议,在设计军事改革的方案时,应把保障信息安全和实施信息对抗这一特殊的领域考虑进去,并作为未来一种重要的武装斗争手段。在对付信息战方面,俄军提出了以下几种措施。

### 3.1 成立信息安全与信息对抗领导、协调机构

俄军认为,统一领导信息战的跟踪研究,并协调有关保护信息安全与反信息战的部门的活动,必须成立高层次的领导机构,该机构在级别上应该相当于俄联邦部一级,该机构掩负责“汇集与信息战有关的一切信息”,并领导和协调有关活动。目前,俄已成立了这种性质的机构,它隶属于总统的国家信息政策委员会,下一步还计划建立相应的职能机构。

### 3.2 制定抗击信息侵略的理论原则

俄军认为,目前俄对信息对抗的研究尚处于初始阶段,虽然已有一些实践,但尚未形成一套完整理论,因此必须组织有关研究机构和部门制定相应的理论,并在此基础上制定“信息对抗构想”。俄军认为,该构想应当阐明:信息威胁的性质;信息对抗的概念;信息对抗的范畴;信息对抗的任务;实施信息对抗的原则;实施信息对抗的程序;信息对抗的组织、指挥方法;信息对抗的发展趋势等。为保证这一任务的落实,俄军认为,必须抓紧培养高水平的信息战理论专家和专业人材。

### 3.3 建立信息对抗心理教育防范体系

俄军认为,稳定国民、武装力量的心理状态,使之无论在平时还是在战时都能经受得住各种严峻的考验,是抗击信息打击的一个重要前提。针对西方把信息心理攻击作为信息战的主要手段的情况、俄军学者认为,必须在全国范围内,特别是在武装

力量和其他专政部门内建立全新的“信息对抗、信息心理对抗教育和防范体系”。这一体系应包括技术防护、宣传解释、思想教育等,特别强调应重视对公民和全体军人进行爱国主义、民族凝聚力的教育。

### 3.4 建立专门对付信息战的特种部(分)队,采取对抗敌信息打击的主动攻击措施

俄军认为,为有效地保障信息安全,确保在信息对抗中保持主动,必须建立特种部(分)队和其他从事信息安全保障的专门组织。此外,还必须研究先机制敌的主动性信息攻击措施,包括对敌指挥系统的计算机网络实施攻击,以破坏、篡改或阻塞其网络中的信息,致使对方瘫痪;对敌指挥系统和信息武器实施人力突击、电子突击,以及其他主动攻击手段。

### 3.5 发展对付信息打击的关键技术和手段

俄军认为,在信息技术特别是军用信息技术的发展方面,俄虽然在整体上落后于美国和其他一些西方国家,但俄已经具有了相当的基础,在某些方面俄军并不落后,只是“尚未形成体系”。在目前经济能力有限,尚不能集中财力、物力大力进行信息化建设的条件下,为了迎接信息地挑战,俄军认为,应着力发展关键技术和手段。专家提出的重点发展领域包括:战略和战场 C<sup>3</sup>I 系统:战略防御体系的信息系统;电子对抗系统:武器平台控制系统。俄军提出重点开发的关键技术包括:高性能计算机技术;智能化技术;信息攻击与防护技术;相关的软件技术等。

### 参考文献

- [1] 徐小岩等.《信息作战学》.北京:解放军出版社,2002
- [2] 伍仁和.《信息化战争论》.北京:军事科学出版社,2004
- [3] 刘桂芳等.《高技术条件下的 C<sup>4</sup>ISR-军队指挥自动化》.北京:国防大学出版社,2002
- [4] 《武器装备的信息化》.北京:解放军出版社

### 作者联系方式

通信地址:北京南口 61622 部队机电教研室  
 邮政编码:102202  
 联系电话:010-66755056 010-69784331

# 构建军用软件体系的多视图研究模型

彭治宇 甄理

**摘要：**随着军队信息化建设的深入，军队软件的研制和应用日趋普遍，为了加强军用软件建设的统筹规划和管理，需要研究建立起军用软件体系。这项研究起步已有一段时间，研究的方法也各有不同，为了适应更高的应用需求，本文提出另一种体系研究的方法，构建出多视图格局的研究模型。

**关键词：**软件体系；信息化；模型；框架

经过多年的努力，我军的信息化建设取得了很大的成绩，一大批军事应用软件相继研制成功并推广应用，大大提高军队机关和部队的作战指挥和日常业务信息处理的时效和质量。但随着建设的深入，军用软件的研制和应用有不少问题就需要进一步研究解决，如总体规划不够、立项开发混乱、应用管理无力、整体效益较低等。为加强军用软件开发与应用的统筹规划和管理，我军越来越认识到建立起军用软件体系的重要性，并开展了广泛地研究。但是，这项体系研究工作本身就具有相当的复杂性，需要采用有效地研究方法，建立的软件体系既要能为业务部门提供软件建设的规划、又要能为技术部门提供科研开发和推广应用的指导。

## 1 研究现状

通常的一种研究方法是，套用军队的编制体制，将软件按军队的编配层次、应用业务、军兵种等方式分类，形成多维的矩阵式框架。这种研究方法的优点是软件与军队的各级各部门对应明确；缺点是软件分类和功能交叉重复严重，形成若干个“烟囱”式系统软件，难以实现各系统软件的复用和互连互通。在信息化建设初期，这种研究方法对各级各部门的分工建设起到了很好的指导作用，但随着信息化建设一体化的深入，军队软件开发与应用越来越强调综合集成程度高、研制开发时效快、互连互通性能好，因此必须有更科学合理的分类方法建立软件体系。

目前，我们已经意识到了从作战体系结构、系统体系结构、技术体系结构三个方面，进行分类研究软件体系。通常的定义为，作战体系结构是指作

战体系的基本框架，反映同类作战体系的通用内容；系统体系结构是指为保障和支持作战功能，各系统及其相互连接的描述；技术体系结构是指为保证一致性的系统满足一组特定需求，支配各部分或各要素配置、相互作用和相互依存的一组最小规则集，支配系统实现和动作的一组规则。

## 2 建立视图研究的模型

可以看出，作战体系结构、系统体系结构和技术体系结构的三个方面，分别对应了军事人员、系统设计人员和技术开发人员的三类人员看待软件体系的角度，由此我们可以建立起“视图”的概念，即不同人员从不同角度看待同一事物，而各自得出对事物的描述。这种系统分析方法，是将复杂问题逐层剖析为简单问题的有效手段。视图与视图之间再建立起内部的对应关系，那么，该事物就能被立体的描述出来了。

在此，可以对军事人员建立军事应用视图，对系统设计人员（或者是业务部门负责信息化建设的人员）建立系统应用视图，对技术开发人员建立技术实现视图。例如军事上的战场态势处理，从军事应用视图来看，包括有部队态势处理、海上态势处理、空中态势处理、电子对抗态势处理等；从系统应用角度来看，包括有地理信息功能、态势标绘功能、目标查询功能、态势综合功能等；从技术实现角度来看，包括有地理信息技术、图形处理技术、实时传输技术、数据库技术等以及部队、舰艇、飞机、电磁等作战计算模型。战场态势处理在各视图中均有映射对应。这样一来，软件体系框架将不再被描述为一个简单地纵横交错的矩阵立方体。

2.1 军事应用视图

建立该视图的军事人员，基本上是不需要具备信息化建设的理论和计算机应用的知识，他们只要将军事领域的各种作战行动和其他相关活动尽可能细致地分解，某个作战行动或活动是由若干个行为组成。例如，部队机动行动可以分解为装载、行进等行动组成，对这些行动再细分就有，装甲车辆的陆上装载、水上装载、空中装载等，山地行进、水网地带行进、呈战斗队形行进等行为动作。因此，采用“行为”的概念来作为描述军事应用视图的基本构建单元，多个行为组合成一个作战行动，多个作战行动又可以组合成更高层次的作战行动，从而可以形成军事应用视图的框架（如图 1）。需要指出，多个作战行动中可能包含同样的行为，如部队机动的行进，和战斗中的行进有共同的行为。

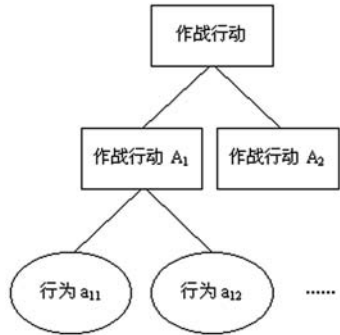


图 1 军事应用视图框架示意图

军事应用框架用集合描述时，军事应用用  $M$  表示，作战行动用  $A_i$  表示，行为用  $a_{ij}$  表示，若军事应用视图共有行为单元  $n$  个，则有

$A_i=\{a_{i1}, a_{i2}, \cdots, a_{ij}\}, j\leq n$ 。当中可能存在这种情况：在  $A_1$  和  $A_2$  中，有  $a_{11}=a_{21}$ 。

$M=\{A_1, A_2, \cdots, A_i\}$ 。

2.2 系统应用视图

建立该视图的系统设计人员，需要具备一定的军事应用知识和技术知识，他们需要将军事应用视图中的各个行为，按功能组成进行转换和分解，对功能相同的部分进行合并。又如部队装载，不管是何种部队、何种装备，从功能来看，就是装载物的体积、重量、形状等计算和承载容器的容量、载重量、形状等计算。因此就有，将不同的装载物计算和承载容器计算组合在一起，就能实现不同部队采用各种运输工具进行装载的计算。如此一来，就能

够实现功能的复用（举例中的各种装载物计算和承载容器计算就可以复用）。系统应用视图就是要将功能分解到最小化，即形成若干个功能模块，模块与模块之间尽量是低耦合；同时描述出各功能模块之间的关系，主要是信息流关系；多个功能模块可以组合成某个应用功能，多个应用功能又可以组合成更高层次的应用功能，这种组合就是集成。由此可以形成系统应用视图的框架（如图 2）。

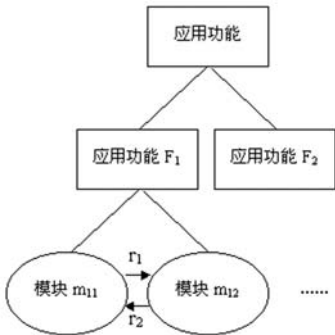


图 2 系统应用视图框架示意图

系统应用视图用集合描述时，系统应用视图用  $S$  表示，应用功能用  $F_i$  表示，功能模块用  $m_{ij}$  表示，若系统应用视图共有功能模块  $n$  个，模块  $m_{ij}$  与  $m_{ik}$  之间的关系用  $r(m_{ij}\rightarrow m_{ik})$  表示，则有

$F_i=\{m_{i1}, m_{i2}, \cdots, m_{ik}, \cdots, m_{ij}, r(m_{i1}\rightarrow m_{i2}), r(m_{i2}\rightarrow m_{i1}), \cdots, r(m_{ik}\rightarrow m_{ij}), r(m_{ij}\rightarrow m_{ik})\}, k, j\leq n, k\neq j$ 。当中可能存在这种情况：在  $F_1$  和  $F_2$  中，有  $m_{11}=m_{21}$ 。

$S=\{F_1, F_2, \cdots, F_i\}$ 。

与军事应用视图存在有对应关系是： $A_i=\{F_j\}$ ，即军事应用视图中的某个单元是由系统应用视图中的若干单元组合而成。当然，在此组合之后可能还要在各单元之间产生新的关系（这里是功能交互关系），此时有  $A_i=\{F_j, R_k\}$ ， $R_k$  是表示  $F_j$  之间的关系。

2.3 技术实现视图

建立该视图的技术人员，主要是将系统应用视图中的各功能模块和关系进行技术实现，这就需要明确算法、数据结构以及数据传递的内容和方式等。在这个视图里，技术人员采用构件化技术方法，将功能模块分解为若干个构件的组合，构件内部具有算法、数据结构和数据传递的接口。构件的建立是将现实世界的实体进行高度的抽象，例如前面说到的装载物，在构件建模里，抽取与装载有关的各实体共有的属性如名称、体积、重量、形状

等，形成实体模型；抽取与装载有关的计算和军事规则，形成算法模型；给定实体的参数，通过模型之间的交互，就能实现给定实体的装载计算功能。除了完成对功能模块的技术转化处理，为支撑技术的实现，技术人员还要解决技术的各种支撑问题，这就要考虑系统环境（如操作系统、安全保密环境等）、服务支持（数据库服务、Web 服务等）、应用支持（如数据传输、图形处理平台等）等，将这些支撑要素和构件组合起来，得到技术实现视图（如图 3）。

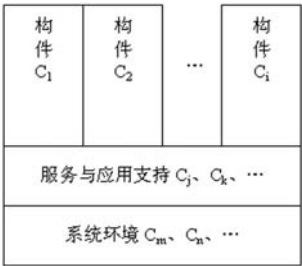


图 3 技术实现视图框架示意图

与系统应用视图存在有对应关系是： $F_i=\{C_j\}$ ，即系统应用视图中的某个单元是由技术实现视图中的若干单元组合而成。当然，在此组合之后可能还要在各单元之间产生新的关系（这里是接口调用关系），此时有 $F_i=\{C_j, T_k\}$ ， $T_k$ 是表示 $C_j$ 之间的关系。

2.4 各视图之间的联系

从军事应用视图到系统应用视图、到技术实现视图，是从现实反映到技术实现的过程，是从具体到抽象的过程。军事应用视图中的每个单元，是系统应用视图中的若干单元的组合实现；系统应用视图中的每个单元，又是技术实现视图中的若干单元的组合实现。从以上的集合公式来看，能够得出

$$M=\{A\}=\{ (F, R) \}=\{ ((C, T), R) \}。$$

2.5 视图的实例化应用和实例视图

从上面的公式中看到，军事应用视图的行为单元最终是由高度抽象了的功能模块和构件组合而成

参考资料（略）

作者联系方式

通信地址：江苏省南京市黄埔路 3 号指挥自动化工作站  
邮政编码：210016  
联系电话：025-80881591

的。那么要实现一个具体的军事应用，就需要对模块和构件进行实例化，通过引入具体的数据，建立起实例视图（如图 4）。

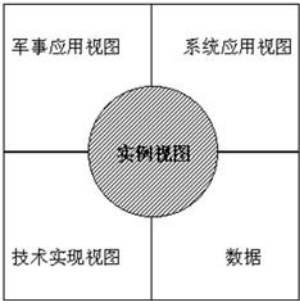


图 4 视图实例化示意图

军事应用视图、系统应用视图、技术实现视图和实例视图的合成，形成了软件体系研究的全视图，实现软件体系的完整描述。

3 采用视图模型研究的优点

采用视图模型建立软件体系研究方法带来如下好处。

1) 将研究的问题进行了层次化处理。由于军事人员、系统设计人员和技术开发人员在认知上具有局限性，只掌握了解各自领域的内容，因此按不同视图对软件体系进行描述，有利于不同类型的人员进行研究分析。

2) 建立了多视图的体系框架。军事应用视图的框架能够为军队业务部门提供软件建设的规划，系统应用视图和技术实现视图能够为技术部门提供科研开发和推广应用的指导。软件体系在使用中，能够分解为各种视图，方便不同类型人员阅读和使用。

3) 建立了各视图的联系。软件体系的各视图是一种多对多的映射关系，克服了由采用传统分类研究方法导致建立起矩阵式关系的弊端，更能体现软件体系的内在结构和关系；同时，由于高度的模块化分解和构件化技术实现，能够实现系统软件的功能复用和互连互通。

# 空军信息资源的层次结构与共享分析

邵志平 周中平

**摘 要：** 本文在研究空军信息资源层次结构的基础上，对空军信息资源的共享需求与数据集成问题进行了较为详细地分析，并就空军信息资源的数据环境重建提出了相应看法。

**关键词：** 信息资源；层次结构；共享需求；数据集成

随着空军信息化建设的展开和人们认识上的深化，信息资源的地位与作用越来越被引起高度的关注和重视。深入开发和广泛利用信息资源，使其充分发挥作用并产生出巨大的军事效益，无疑是空军信息化建设的核心任务和源头性工作。由于空军是一个多兵种、多专业力量组成的合成军种，客观上决定了空军信息资源的共享问题十分突出。因此，建立一个科学合理的信息资源共享机制，是有效地消除空军内部信息“壁垒”，盘活信息资源的前提，也是实现空军信息化作战能力全面提升的一项基础性工作。

建立科学合理的空军信息资源共享机制，依赖于对空军信息资源的层次模型与共享问题的准确理解和把握。本文将就这一问题进行初步探讨。

## 1 空军信息资源的层次结构

信息，在拉丁语词源中是通知、报导或消息的

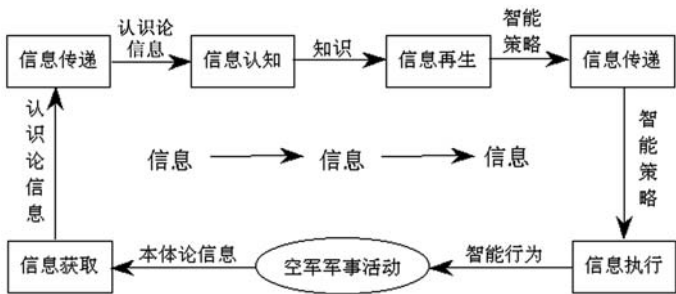


图 1 空军信息资源的开发利用

在空军信息化建设过程中，信息资源的开发利用既包括了从外延上发掘信息来源、开拓信息渠道、建立信息库存、加速信息流动的过程；又包括了从内涵上不断重组和加工信息内容的过程；还包括了有目的、有选择地、能动地运用信息的活动。显然，空军信息资源是一个多层次、多目的、多用

意思；在日常生活中，信息则被理解为消息。这是关于信息的感性认识。对于信息的理性认识，消息只是信息的外壳，信息则是消息的内核。从哲学本体论上讲，信息是事物运动状态及其状态变化方式的描述；从认识论层次上讲，信息是认识主体所感知或表述的事物运动状态及其状态变化的方式。人类认识世界的任务和先决条件之一，就是要把本体论信息恰如其分地转化为认识论信息，为其后决策提供依据。

基于以上认识，空军信息资源的开发利用，实质上是一个信息获取、信息传递、信息认知、信息再生和信息执行的过程（图 1）。其根本目的就是要将空军军事活动中的本体论信息恰如其分地转化为认识论信息，为空军各级指挥员和司、政、后、装部门领导提供决策支持，并在空军部队作战行动和日常管理过程中有效地发挥作用。

途的有机整体。为了清晰地反映空军信息资源的层次结构，可以将其分为基础信息、业务处理信息、决策支持信息和作战应用系统信息四个层次（图 2）。

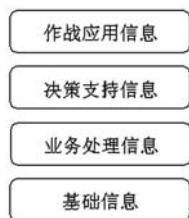


图2 空军信息资源的层次结构

基础信息，是指可供诸军兵种共同使用的地理环境、大气环境、外层空间环境等战场环境的基础数据。基础信息生成后，大多在几年甚至几十年内不会发生变化。因此，信息更新频率要求不高，甚至可以不进行定期更新，只需要在信息发生变化时才进行修改。

业务处理信息，是指空军各级司、政、后、装机关在组织部队作战行动和日常管理过程中，通过各类感知系统实时收集、处理并循环使用的相关业务信息。业务处理信息通常是初步的、原始的数据集合，不能由其他信息导出。在空军信息资源的层次结构中，业务处理信息与基础信息的粒度同时达到最小，是空军体系正常运转的基础，也是空军各级各类信息系统的重要信息来源。

决策支持信息，是指通过对基础信息和业务处理信息进行综合加工后得到的、能够辅助空军各级指挥员和司、政、后、装部门领导进行决策的信息。决策支持信息在决策者（人或机器）的智能化思维过程中形成，实现了信息资源从“可以做”向“应该做”的结论转化。其决策支持作用，不在于确定决策方案的可行与否，而在于决策者没有预见到时候就已经提出了可行的方案。在空军信息资源的层次结构中，决策支持信息的粒度最大。

作战应用信息，是指在空军信息化作战过程中，按照智能策略形成智能行为的武器控制信息与作战协同信息。作战应用信息实际上是决策支持信息的一种状态转换，具有极强的目的性，直接决定着信息资源的利用效率和信息作用的有效发挥。因此，作战应用信息处于空军信息资源层次结构中的顶层，也是牵引空军信息资源开发利用的核心因素。

## 2 空军信息资源的共享需求

空军信息资源共享的最终目标，是彻底消除空军内部的“信息孤岛”，打破部门之间的信息

“壁垒”，使空军体系运转中源源不断产生的信息资源充分发挥作用，并产生出巨大的军事效益。

由于空军信息资源分散在各级部门，信息种类形式多样，数据结构千差万别。这些种类繁杂的信息，采用完全集中的方式在技术和管理上是不可行的，而采用完全分布式的管理方式也存在协调、控制、综合集成等方面的诸多问题。因此，必须建立集中和分布相结合的信息资源共享体系。考虑到空军体系的运转机制和信息资源的分布状况，空军信息资源的共享需求主要是从纵向和横向两个方面来把握。

从纵向上看，空军信息资源的共享主要是业务处理信息的共享。目前，空军大多数业务处理信息的流动是从基层部队（分队）上报区域指挥所（或师、旅、团），区域指挥所（或师、旅、团）汇总后上报军区空军，军区空军汇总后上报空军。由于各级上报的信息内容基本相同，因此，基层部队（分队）上报的信息可以直接放在区域指挥所（或师、旅、团）业务信息系统数据库中，下级业务部门上报的信息也可以放在上级相应的业务信息系统数据库或者数据仓库中，以便上级业务部门统计分析和综合处理。空军信息资源共享需求纵向分布模型如图3所示。

从横向上看，空军信息资源的共享主要是基础信息和作战应用信息的共享。同时，空军各级机关的不同业务部门之间为了更好地协作，其相应的业务处理信息和决策支持信息也需要共享。目前，空军各级机关的不同业务部门之间的信息共享，主要是通过直接的横向网络操作实现，无需通过各自的顶级数据源获取。这种方式交互网程短、速度快，但是在保证信息安全可靠性方面和数据接口设计上比较复杂。空军信息资源共享需求横向分布模型如图4所示。

基于空军信息资源的共享目标和需求分析，综合考虑空军信息资源四个层面的共享需要，可构建空军信息资源共享的集中分布式模型如图5所示。该模型包括“空军信息资源共享网络”和“空军信息资源共享服务”两部分，其中，“空军信息资源共享网络”是实现信息资源共享的硬件基础，分为纵向和横向两部分网络互联；“空军信息资源共享服务”是从数据组织、数据库管理方面描述实现信息资源共享的软件要求。



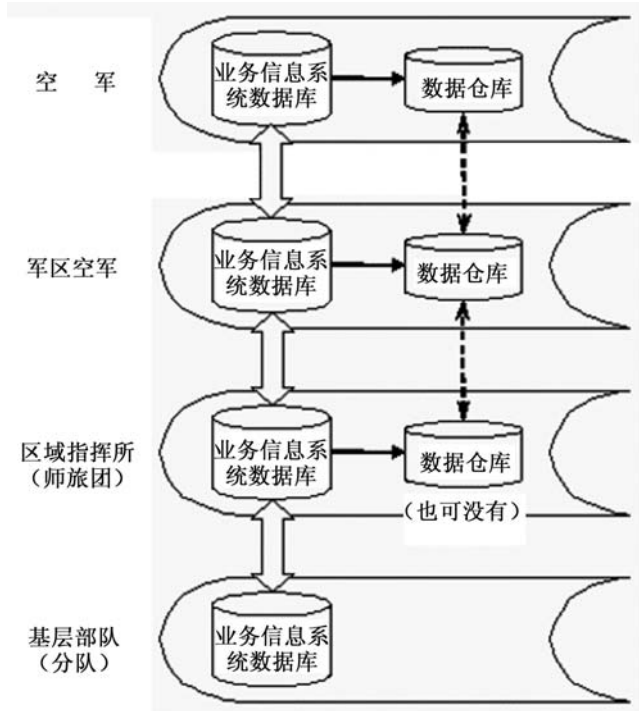


图3 空军信息资源共享需求纵向分布模型

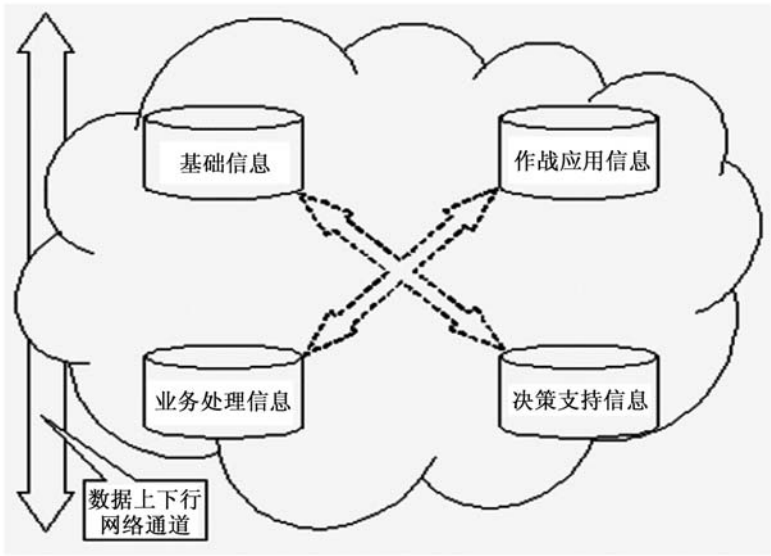


图4 空军信息资源共享需求横向分布模型

目前，全军指挥自动化网和综合业务信息网的建设为空军信息资源共享网络提供了很好纵向互联的网络硬件支撑，而空军各级建立的内部网络则能够较好地提供本级横向互联的需要。构建空军信息资源共享的集中分布式模型，就是要通过对现有的纵横网络关系进行合理整合，建立一个纵向有序互

通、横向有序互联的空军信息资源共享网络。空军信息资源共享服务的最终目标，是在空军信息资源共享网络的硬件环境基础上，建立覆盖空军各级种类应用系统的信息资源共享服务，实现数据的分级式管理和集成式共享，辅助空军各级指挥员和司、政、后、装部门领导进行科学地决策。

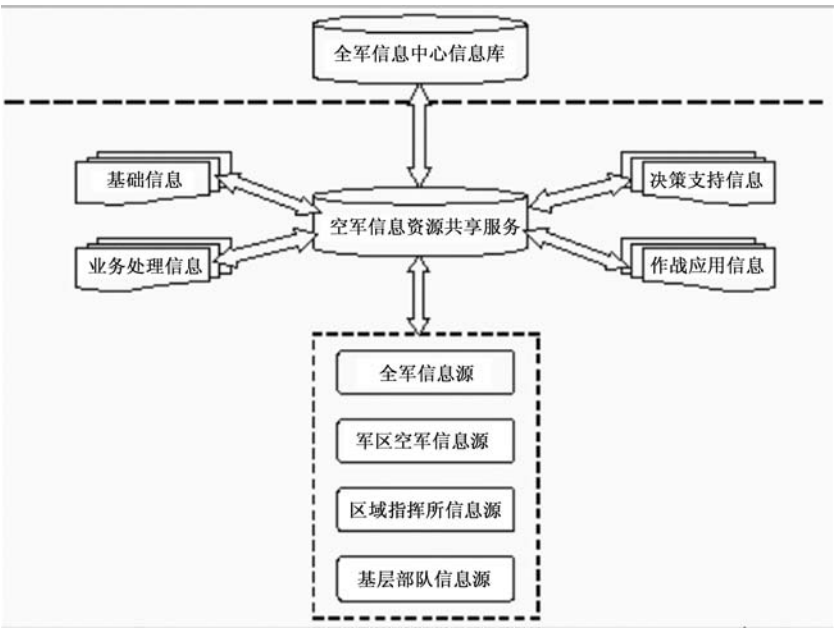


图 5 空军信息资源共享的集中分布式分布模型

3 空军信息资源共享中的数据集成

在空军信息资源的开发利用中，面临的一个最大难题就是许多业务部门分散开发的各种应用系统的信息共享问题。这些所谓的信息系统，实际上是一些互不关联的数据结构（数据文件和应用数据库）和一些应用程序的堆砌。

由于每个应用系统所存储、变换的冗余或重叠的数据紧紧交织在一起，要修改或扩充这些系统的任何部分，都是十分困难和代价高昂的。为了降低信息资源开发利用的成本，不少部门期望通过建立“数据接口”的方式来实现各种应用系统的综合集成。这些“数据接口”，实际上就是针对不同数据所建立的对照转换表。然而，通过数据接口来解决空军现有信息资源的共享问题，只能是一种可望而不可及的设想。如果假设每个应用系统中只有一个数据存储（实际情况是一个应用系统使用多个冗余的数据存储），表 1 列出了为连接孤立应用系统所需要的数据接口数目，这些接口的数目和复杂性随着应用系统数量的增加按非等比级数增加。显然，通过数据接口来实现信息共享，当孤立的应用系统数目较多时，即使系统集成后能够运行，由于各数据存储间频繁地相互转换，也是低效率和脆弱的。

由此可见，空军信息资源的开发利用，实际上是一种空军信息资源的数据环境重建工程，其实质就是数据的集成。重建空军信息资源的数据环境，

理想的情况是把空军各级业务部门的所有应用系统都建立在统一的、高档次的数据环境之上，称之为“全域集成”。但是，在现有条件下，实现“全域集成”的难度很大，所需时间也较长。与之相对应，实现局部集成的难度则较小，所需时间也较短。

表 1 连接孤立应用系统所需的接口数目

应用系统数量	数据存储数	可能的接口数
1	1	0
2	2	2×1=2
3	3	3×2=6
4	4	4×3=12
5	5	5×4=20
6	6	6×5=30
7	7	7×6=42

在现阶段，空军信息资源的数据环境重建工程，应该通过总体数据规划，进行空军共享数据库的重新设计，有步骤地实现对所有数据定义（包括数据定义的安全性、备份、恢复和所有修改的跟踪检查）的集中控制与管理，最终建成面向业务主题、各个应用系统“共建共用”的数据组织与存储环境。

目前，空军各级业务部门大都建有自己的应用信息系统。这些应用信息系统中，有些是为专门业务需要设计的，有些则是在若干相关业务部门之间同时使用的。数据集成的任务，就是将各个不同

的应用信息系统的数据库的数据根据需要导入共享数据库中，同时在保持数据一致性地基础上减少数据冗余。除了个别成熟的应用系统可使用少量非过渡性的数据接口实现连接外，空军各级内部的数据交换应尽可能通过共享的数据库存取数据，避免使用数据接口。

根据空军信息资源的数据环境现状，数据集成过程主要由四部分组成（如图 6 所示）。即：从应用信息系统到本级数据中心共享数据的集成；从下级数据中心共享数据到上级数据中心共享数据的集成；从共享数据到决策支持数据的集成；从应用信息系统到决策支持数据的集成。

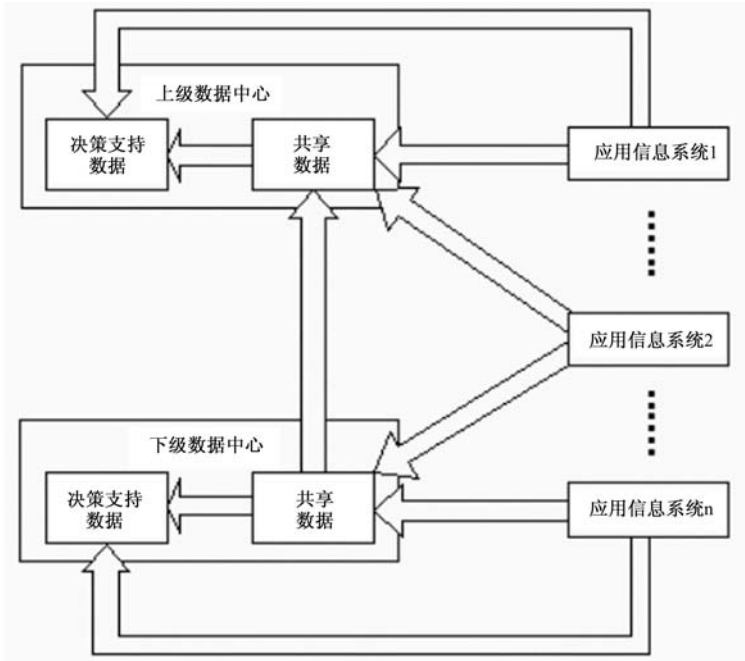


图 6 空军信息资源共享的数据集成过程

参考文献

[1] 吕新奎.《中国信息化》. 北京：电子工业出版社，2002  
[2] 潘明惠.《信息化工程与应用》. 北京：清华大学出版社，2004  
[3] 高复先.《信息资源规划—信息化建设基础工程》. 北京：清华大学出版社，2002  
[4] 李学伟.《中国铁路信息资源理论基础》. 北京：清华大学出版社，2004

作者联系方式

通信地址：北京市海淀区北四环西路 88 号空军指挥学院指信教研室  
邮政编码：100097  
联系电话：010-66924115    010-66923572

# 树状信息化建设项目评估体系浅探

隋晓斐 王艳梅 付楚胜

**摘 要:** 军队信息化建设的推进使得信息化建设项目越来越多,盲目地建设信息化项目不仅浪费钱财,更会贻误信息化建设的大好时机。所以作者提出建立信息化建设项目评估体系,对项目进行定量评估筛选。该体系采用树状架构,更加符合我军信息化实际。

**关键词:** 信息化; 树状; 项目评估

随着部队信息化建设的不断推进,部队里各种信息化建设项目也是越来越多。由于我军信息化建设中存在国防经费有限、信息化建设摊子大、基础差的实际情况。因此,信息化建设项目不能盲目上马,要根据领导机关重点突破、作战部队局部突破、基层单位分步突破的原则,经过科学评估保证关键项目优先发展才能在最短的时间内产生最大的军事效益,在有限的条件下最大程度地提高我军信息化整体实力。所以有必要建立一套科学合理的信息化建设项目评估体系。为此结合我军信息化建设实际,本文提出了树状信息化建设项目评估体系。

世界上只有美、英、俄、中、韩、澳、哈佛大学与世界经济论坛等少数国家和组织建立起了信息化水平评估体系,但该体系是对整个国家的信息化水平的高低进行评估。目前并没有可以针对单个军队信息化建设项目是否该建进行评估的评估体系。作者提出的树状信息化建设项目评估体系,是采用自顶向下的设计思想逐步把量化指标进行细化,从而可以从各个方面对某个信息化建设项目进行全面定量评估的评估体系。

## 1 树状信息化建设项目评估体系的可行性

一是更加科学合理。评估体系构成要素的确立必须经过各方面的专家论证才能完成。但是专家限于其研究领域的不同不能对整个体系都了然于胸。采用树状结构对评估体系的各个指标进行分级,首先由总体规划专家确定第一级指标的分类及权重,然后各方面的专家分别对第一级中的某一指标进行分类细化,确定权重。通过自顶向下的逐层细化,既能做到指标构成要素不缺失不遗漏又能保证评估体系客观准确。另外,初步制定的评估体系不可能

十全十美,必须要随着实践的深入和信息技术的进步对评估体系进行不断的修改。采用树状评估体系,可以在保留大块评估体系的情况下只对相应级别的某一组或一个指标进行修改,修改比较方便。

二是适合现有军情。信息化建设需要全军各级部门共同努力,按照各自的分工和建设重点密切配合,协调发展。树状评估体系可以使各级按照评估体系相应层次确立自己的任务。各级只需对评估体系的某一块进行重点关注即可,避免了囫圇吞枣的“消化不良”现象。另外,对信息化建设项目进行评估必然需要大量的数据信息,而军队的数据信息有很多是保密的。采用树状评估体系,各级只需知道相应级别的数据信息即可,缩小了信息接触范围。这样既避免了数据信息的泄密又能保证评估的真实准确。

## 2 树状信息化建设项目评估体系的指标分类

考虑我军实际,树状评估体系采用三级结构。通过研究,笔者对树状评估体系的各级构成要素提出了自己的看法。如表1所示。

对项目评估体系采用了下述分法主要是因为,信息化建设项目必须要符合国家和军队的总体发展要求,同时又不能脱离军队的实际情况,所以评价体系要建立规范性和适应性指标;信息化建设项目不能走重复建设、低层次建设的路子,关键技术必须掌握自主产权,不然仍会受制于人,以经济建设为中心的总体的国策要求军队经费不能无限制增长,所以要建立技术性指标和经济性指标;建设信息化项目目的是为了得到或增强各种信息化的能力,所以效能指标更是不能缺少的关键指标。

表 1 树状评估体系的各级构成要素

信息 化建 设项 目评 估体 系	第一级	第二级	第三级
	与 现 有 环 境 适 应 度	政策、标准、法规	符合国家、军队政策度
			符合国家、军队法规度
			符合发达国家标准度
		体制、编制	符合各军种体制编制度
			符合联合作战要求度
		与基础设施匹配情况	与信息栅网匹配度
			与传感器网匹配度
			与现代武器网匹配度
	技 术 情 况	信息技术发展程度	技术的领先程度
			技术的成熟度
			自主知识产权情况
		项目初步可行性	安全可靠度
			经济可承受度
	信 息 化 效 能 情 况	提高武器装备信息化程度	武器装备信息化改造程度
			引入武器装备的信息化程度
			提高武器装备的互联互通程度
		提高人员信息化素质程度	提高新信息化知识程度
			提高操作信息化武器装备能力
			提高信息化应用能力程度
		提高信息化作战能力程度	提高联合作战能力程度
			提高夺取制信息权能力程度
			提高利用信息能力程度

3 树状信息化建设项目评估体系的计算方法

树状信息化建设项目评估结果可以用如下公式计算：

point=∑<sub>i=1</sub><sup>n</sup>[∑<sub>j=1</sub><sup>m</sup>(∑<sub>k=1</sub><sup>l</sup>P<sub>ijk</sub>W<sub>ijk</sub>)×W<sub>ij</sub>]×W<sub>i</sub> (1)

其中，point 代表信息化建设项目的最终评估得分；n、m、l 分别为指标体系第一、二、三级指标的个数；p 为第三级评估指标某一要素的值（表 3）；w 为某一要素的权重（表 2）。心里学家的研究提出：人们区分信息等级的极限能力为 7±2。作者据此制定了表 2 和表 3。结合表 2 和表 3 采用专家打分的方法确定 W 和 P 的值：采用调查问卷方式，分别请研究该问题的有关专家为某个指标的权重和效能进行打分，将多个专家打的分数进行平均后分别作为权重和效能的值。得到值后代入公式（1）中，得到 point 的值越大代表该项目越科学，越符合军队信息化发展的趋势，越应该优先发展。

表 2 信息化建设项目的权重描述

W 值	定义
1	该要素一般重要
3	该要素略重要
5	该要素较重要
7	该要素非常重要
9	该要素绝对重要
2, 4, 6, 8	为以上两判断之间的中间状态对应的标度值

表 3 信息化建设项目的指标值描述

P 值	定义
1	基本不能提升信息化能力
3	可以略微地提升信息化能力
5	可以较大地提升信息化能力
7	可以非常大地提升信息化能力
9	可以极大地提升信息化能力
2, 4, 6, 8	为以上两判断之间的中间状态对应的标度值

例如：某一项目假设经过专家打分后，第一级指标“技术情况”的权重值 W<sub>2</sub> 为 7，它下面的两个二级指标“信息技术发展程度”“项目初步可行

性”的权重值  $W_{21}$ 、 $W_{22}$  分别为 8、9，第三级指标“技术的领先程度”“技术的成熟度”“自主知识产权情况”“安全可靠度”“经济可承受度”的权重值  $W_{211}$ 、 $W_{212}$ 、 $W_{213}$ 、 $W_{221}$ 、 $W_{222}$  分别为 7、5、6、9、4，这五个三级指标最后的得分  $P_{211}$ 、 $P_{212}$ 、 $P_{213}$ 、 $P_{221}$ 、 $P_{222}$  的值分别为 6、7、4、5、3，则代入公式（1）

$$[(P_{211} * W_{211} + P_{212} * W_{212} + P_{213} * W_{213}) * W_{21} + (P_{221} * W_{221} + P_{222} * W_{222}) * W_{22}] * W_2$$
 结果为 9247，按照同样的方法再计算出其他两个一级指标的

得分并与 9247 相加，就得到这一项目的最后得分。

军队信息化的前进步伐已不可阻挡，信息化建设项目评估体系在信息化建设中的地位和作用越来越突出。当前首先要解决的是有无问题，然后在实践中再去解决评估体系的完善问题。所以只要评估体系具有一定的综合性、可操作性和导向性，基本符合我军需求即可。本文正是本着这一原则，从需求分析和可行性入手，提出了三级树状评估模型。只要不断地加以完善，该评估体系必定能为我军的跨越式发展发挥巨大力量。

### 参考文献

- [1] 《运筹学》. 北京：清华大学出版社，2005.6
- [2] 韩彬霞，何集体，勾军辉.《信息技术与现代武器融合的基本构想》2003
- [3] 赵弘.《建立具有我军特色的信息化指标体系浅探》，2003
- [4] 杨耀辉.《军队信息化测评探索》，2003
- [5] 孙海成，刘汉民，季士东，赵弘.《对军队信息化建设若干问题的思考》
- [6] 总参通信部.《我军信息化建设探索》2003.5

### 作者联系方式

通信地址：武汉市二七路 145 号二炮指挥学院研管大队一队

邮政编码：430012

联系电话：027-51252689      027-63849636

# 一种改进的网络节点重要度评估方法

孙梅 周万宁 詹武

**摘 要:** 网络的非同质性使得节点重要度的计算具有重要意义。本文介绍了一种基于网络凝聚度的节点重要度评估方法,并针对其局限性提出了一种带标记的节点重要度计算方法。此方法解决了原方法中对某些节点重要度无法区分的不足。运用此方法可以找出网络中的核心节点,从而可对这些节点重点加以维护、进行冗余备份,提高整个网络的可靠性。

**关键词:** 节点重要度;网络凝聚度;节点收缩

## 1 引言

现实生活中的网络大多是不均匀的,或称为“非同质的”。在这样的网络中,有的节点具有大量连接,有的节点(如末梢节点)只具有少量连接,这种网络表现在连接度分布上就是连接度分布曲线是不断递减的。印第安纳州圣母大学物理学教授巴拉巴斯把具有这种性质的网络称之为无标度网络(scale-free networks)。由于具有少量核心节点,无标度网络在遭受智能打击时相当脆弱,因此对核心节点更应做好冗余备份、重点保护工作,从而提高整个网络的可靠性。我们可以通过对网络中各节点重要度进行评估来找出网络中的核心节点,核心节点是网络中占有重要地位的节点,但并不一定是连接数最多的节点。本文介绍了一种基于网络凝聚度的节点重要度评估方法,这种方法以网络凝聚度作为节点的重要度,认为如果某个节点是一个很重要的“核心节点”,那么将它收缩后整个网络将更好的凝聚在一起。此方法综合考虑了节点的度数及其在网络中占据的位置,可以较好地反映节点在网络中的重要性。文中第三部分,分析了此方法存在的不足,进而提出了一种带标记的节点重要度评估方法。第四部分,进行实例演算,验证了改进后方法的有效性。

## 2 节点重要度评估方法

过去人们经常把节点的度数作为节点重要性的衡量标准,认为与节点相连的边越多则该节点越重要。这种评估方法具有一定的片面性,因为有些关

键节点(这里的关键节点指的是许多节点对间的最短路径都要通过的节点)并不一定具有较大的度数。文献[1]提出了基于凝聚度的节点收缩方法来评估网络中的节点重要度。

节点收缩法是每次将某个节点收缩,再计算所得图的网络凝聚度,并以此值作为该节点的重要度。某节点收缩是指将与该节点相连接的所有节点都与该节点短接,即用一个新节点代替这些节点,原先与它们关联的边现在都与新节点关联。相当于该节点将它周围的所有相连的节点“凝聚成了一个节点”<sup>[1]</sup>。如果某个节点是一个很重要的“核心节点”,那么将它收缩后整个网络将更好的凝聚在一起。

网络凝聚程度的衡量标准是节点之间的平均最短路径距离(以  $l$  表示)和网络中的节点数目(以  $n$  表示)。定义网络凝聚度为节点数与平均最短路径乘积的倒数。公式表示如下:

$$\partial = \frac{1}{n \cdot l} = \frac{1}{\sum_{i,j \in V} d_{ij}} = \frac{n-1}{2 \sum_{i,j \in V} d_{ij}} \quad (1)$$

其中  $d_{ij}$  代表节点  $i$  和  $j$  之间的最短距离。显然  $0 < \partial \leq 1$ , 当网络中只有一个节点时,网络凝聚度取最大值 1。

## 3 改进的节点重要度评估方法

上述方法在评估节点重要度时同时考虑到节点的度数和节点所处的位置,相比较原来仅以节点度数作为评判标准来说更能反映网络的实际情况。但在使用时发现,该方法仍具有一定局限性,对有些

节点重要度无法区分。例如图 1，按上述节点收缩法，将节点 1 或节点 8 收缩后如图 2，节点 2、3、4、5、6、7 中任意一个节点收缩后如图 3。按公式 1 可计算出各节点的重要度如表 1。

表 1

节点	重要度
1	5/56
2	2/15
3	2/15
4	2/15
5	2/15
6	2/15
7	2/15
8	5/56

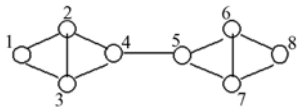


图 1

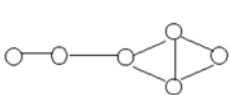


图 2



图 3

从计算结果来看，节点 1 和节点 8 重要度最小，节点 2、3、4、5、6、7 重要度相同，值最大。而我们可以很容易地从图 1 中看出，节点 4 和节点 5 连接两个子网，它们两个中任意一个出现故障将导致两个子网无法互通。而节点 2、3、6、7 中任意一个故障，不会影响网络中其他节点间的通信，重要度显然应该低于节点 4 和节点 5。鉴于此，本文对原有重要度算法进行改进，提出一种带标记的节点收缩法。

所谓带标记的节点收缩法是指，在使用节点收缩法时，用实心圆圈代表收缩后的新节点，计算出收缩后的网络凝聚度，从而得出各节点的重要度。对重要度相同的节点，如果其收缩后的图完全相同，则不再进一步分析。对重要度虽然相同，但收缩后的图不同的还要做进一步分析。我们可以采用三种辅助方法来进一步区分节点的重要度。方法一，比较收缩后图中新节点（即图中实心圆圈）的度数，度数大的所对应节点的重要度更大。方法

二，计算经过新节点的最短路径的数目，数目大的所对应节点的重要度更大。方法三，对收缩后的图再次使用带标记的节点收缩法，计算所得图的网络凝聚度，凝聚度大的所对应节点的重要度更大。

4 实例分析

以图 1 为例，对图 1 进行第一次带标记的节点收缩，节点 1 或节点 8 收缩后对应图 4，节点 4 或节点 5 收缩后对应图 5，节点 2、3、6、7 中任意一节点收缩后对应图 6。计算图 4、图 5 和图 6 的网络凝聚度，得出节点重要度如表 1。对于节点 1 和节点 8，重要度相同，收缩后的图也完全相同，因此不再区分。图 5 和图 6 不同，但节点 2、3、4、5、6、7 的重要度相同，因此应进一步区分节点 4、5 与节点 2、3、6、7 的重要度。

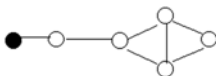


图 4

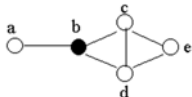


图 5



图 6

方法一，由图 5 和图 6 可看出：图 5 中的新节点度数为 3，图 6 中的新节点度数为 1，应该是节点 4 和节点 5 的重要度高于节点 2、3、6、7。

方法二，计算经过新节点的最短路径的数目。为方便计算，我们对图 5 和图 6 中各节点进行编号。下面列出图 5 和图 6 中各节点对间的最短路径，由于图 5 和图 6 的结构是相同的，只是收缩后新节点的位置不同，因此各节点对间的最短路径表是一样的，如表 2 所示。表中下对角线部分与上对角线部分相同，故不再列出。

表 2

节点	a	b	c	d	e
a		a-b	a-b-c	a-b-d	a-b-c-e
b			b-c	b-d	b-c-e
c				c-d	c-e
d					d-e
e					





由表 2 可得，图 5 中经过收缩后新节点（即 b 节点）的最短路径数是 7。图 6 中经过收缩后新节点（即 a 节点）的最短路径数是 4。因此节点 4、节点 5 对网络凝聚度贡献更大，重要度也越大。

方法三，对图 5 中的 b 节点和图 6 中的 a 节点再次使用带标记的节点收缩法。分别如图 7 和图 8。计算图 7 的网络凝聚度为 1/2，图 8 的网络凝聚度为 3/14。图 7 是由图 1 中节点 4 或节点 5 两次带标记收缩后得到的，图 8 是由图 1 中节点 2、3、6、7 中任意一点两次带标记收缩后得到的，因此可判断节点 4 和节点 5 的节点重要度大于节点 2、3、6、7。

通过这种方法可以更准确地反映网络中节点的重要度，实例证明此方法是有效的。

## 5 结束语

本文提出了一种改进的节点重要度评估方法，即带标记的节点收缩法，此方法解决了原方法对某些节点重要度无法区分的问题，更能切实地反映网络的实际情况。在日常的网络维护工作中，使用该方法可以找出网络中的重要节点，有的放矢地对这些节点进行重点保护、冗余备份，以尽可能减少网络节点故障带来的损失，提高网络的可靠性。

## 参考文献

[1] <<复杂网络可靠性研究>>. 谭跃进. <http://www.skfse.org/whucn/cccn/session/2-1/wj.ppt>

[2] <<A NEW SURVIVABILITY MEASURE FOR MILITARY COMMUNICATION NETWORKS>> Haizhuang Kang, Clive Butler, Qingping Yang, 1998 IEEE

## 作者联系方式

通信地址：北京万寿路 3 号  
邮政编码：100036  
联系电话：010-66974138 13311328952

# 军事信息资源目录体系研究

王军玲 荀静 张红亮

**摘 要：**信息资源目录体系是解决信息资源共享问题的一种有效途径，是当前信息时代一项崭新的课题。本文针对我军信息资源开发与利用的现状，给出了军事信息资源目录体系的基本概念；详细论述了军事信息资源目录体系总体框架及研究内容，并对其应用模式和工作流程进行了描述；最后提出了实现军事信息资源目录体系所涉及的关键技术。信息资源目录体系研究为我军信息资源目录体系建设提供充分的论据和科学的手段与方法。

**关键词：**军事信息资源；信息资源目录体系；信息资源共享

## 1 概述

军事信息资源是由军事部门或者为军事部门采集、加工、使用、处理的信息资源，主要包括军事部门在履行职能过程中产生和生成的信息资源（如会议文件、公文、档案、规划、方案等）、由军事部门投资建设的信息资源及由军事部门授权管理的信息资源（如各类数据库、文件库等）。军事信息资源是军队作战指挥、训练、战备和日常业务处理活动中不可或缺的可用资源，是一种具有重要价值的军事资源。军事信息资源的有效开发和利用，对促进我军信息化建设起着至关重要的作用。

目录是信息组织的一种方式，它根据语法、语义和语用等规则对信息进行组织，以方便信息的检索。不同的信息组织方式构成了目录体系。军事信息资源目录体系是按照统一的标准和规范，将对军事信息资源进行编目，生成军事信息资源目录内容，并为信息资源使用者或应用系统提供军事信息资源的发现和定位服务，即使用者通过军事信息资源目录体系，在一定的权限下，可知道全军都有哪些信息，所需的信息存放在哪里。军事信息资源目录体系是实现军事信息资源共享和交换的前提。

## 2 军事信息资源目录体系总体框架

军事信息资源目录体系总体框架如图 1 所示。军事信息资源目录体系主要由目录内容服务系统、信息库系统、标准与管理规范、网络基础环境和信息安全保障五部分组成。其中目录内容服务系统

和信息库系统构成了军事信息资源目录体系的技术支撑环境。网络基础环境将依托现有军事综合信息网、指挥网等基础网络。信息安全保障将依托全军信息安全保障设施和信息安全服务，如，身份认证服务、授权服务、数据加密服务等。

### 2.1 目录内容服务系统

目录内容服务系统是通过编目、注册、发布、查询和维护信息资源目录内容，向目录使用者提供军事信息资源的发现和定位服务。使用者通过目录内容服务系统，可查询所需的目录信息，并根据目录信息的指引，按照已设定的用户权限，可访问到相关的信息资源。目录内容服务系统由编目子系统、报送子系统、管理子系统和信息服务子系统组成。

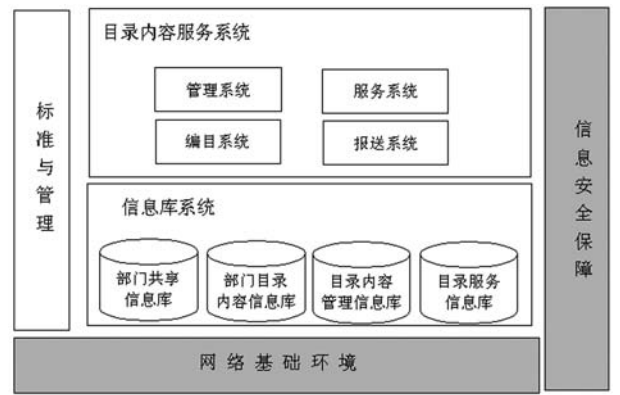


图 1 军事信息资源目录体系总体框架

### 2.2 信息库系统

信息库系统由部门共享信息库、部门目录内容信息库、目录内容管理信息库和目录内容服务信息库组成。部门共享信息库存放的是部门提供的共享

信息资源,包括数据库、网页、电子文件等形态的信息资源。部门目录内容信息库存放的是从部门共享信息库中提取的信息资源的核心元数据。目录内容管理信息库存放的是编目部门向目录中心报送的部门目录内容,目录中心的管理者可对其进行审核与管理。目录内容服务信息库存放的是目录中心发布的目录内容,可供用户查询与检索。其中目录内容管理信息库和目录内容服务信息库部署在目录中心,部门共享信息库和部门目录内容信息库可视具体情况部署在目录中心或各业务部门。

## 2.3 标准与管理规范

制定标准与管理规范是建立军事信息资源目录体系的核心。标准与管理规范主要包括技术标准规范和技术管理要求。技术标准规范通过制定军事信息资源分类标准、军事信息资源目录体系元数据、标识符编码规则等,对军事信息资源目录内容进行了规范,实现对所有的信息资源的统一检索和调度,确保信息的查全率和查准率,以支持业务部门间信息资源的共享。技术管理要求给出建立军事信息资源目录体系的管理规定,包括管理架构、管理角色及其职责、目录体系建立活动等管理要求。技术管理要求将规范相关角色在军事信息资源目录体系建立活动中的行为,规范军事信息资源目录体系建设、运行、维护、服务、安全等方面的管理制度,以确保军事信息资源目录体系的建立和管理工作的有序推进。

# 3 运行描述

## 3.1 应用模式

目录内容的提供者、管理者和使用者是信息资源目录体系中的三种角色。各种角色通过不同的角度,对信息资源进行组织、查找和管理。提供者负责部门目录内容的规划和编目,并保证编目信息的正确性。管理者负责部门目录内容的注册,负责目录中心目录内容的管理和发布以及系统维护,并须保证目录信息的安全。使用者查询信息资源目录内容。

针对不同的角色,目录内容服务系统具有三种

应用模式:生产模式、管理模式和服务模式。

### ● 生产模式

生产模式为提供者提供用于编辑本部门目录内容的服务。

### ● 管理模式

管理模式为目录中心管理者提供的管理界面。其功能是对目录中心管辖的目录内容进行审核、管理和发布。

### ● 服务模式

服务模式为使用者提供的查询和检索各类信息的窗口。用户通过查询所需的目录信息,并根据目录信息的指引,按照已设定的用户权限访问相关的信息资源。

## 3.2 工作流程

目录内容由编目系统产生,报送至目录中心,经过目录中心的审查后,并进行发布,在使用者查询时提供给查询用户。其具体工作流程如图 2 所示。

各业务部门根据信息资源共享和交换的实际需要,将共享信息从部门业务系统发布到信息共享环境;通过编目子系统,提供者(部门信息系统管理员)按照统一的元数据标准、军事信息资源分类标准和标识符编码规则,提取共享信息的主要特征,进行目录内容编辑,形成目录内容,存储到部门目录内容信息库中;通过报送子系统,把部门目录内容汇聚到目录中心的目录内容管理信息库;目录中心的管理者通过管理子系统,对汇聚的目录内容进行审核,符合标准的目录内容自动进入目录内容服务信息库,未通过审核的目录内容自动返回该目录内容提供部门,经修正后,重新审核;使用者通过服务子系统发现和定位所需的信息资源。

# 4 目录内容服务系统

目录内容服务系统由编目子系统、报送子系统、管理子系统和服

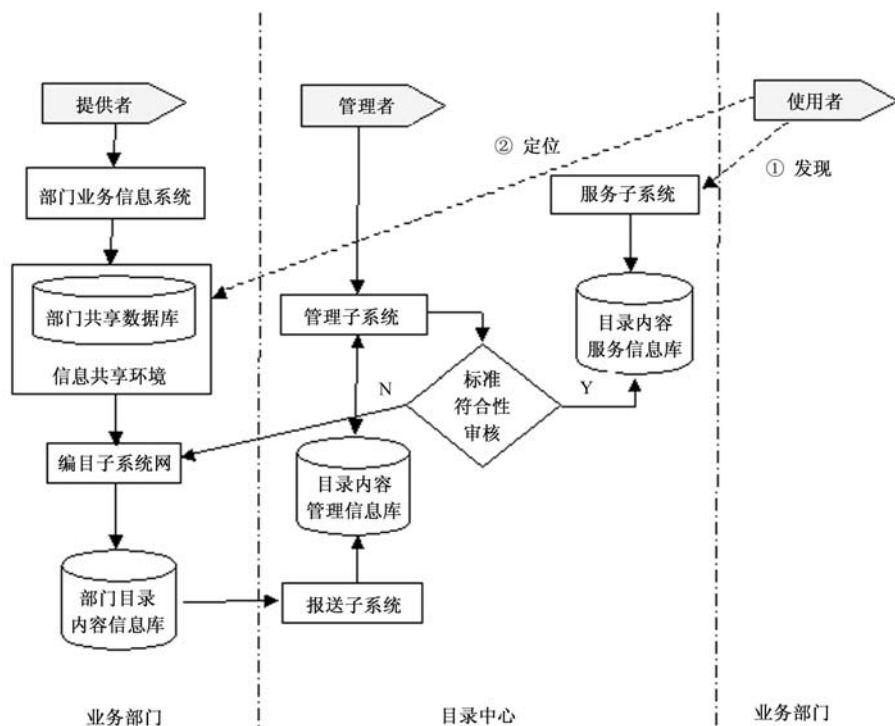


图2 军事信息资源目录体系工作流程

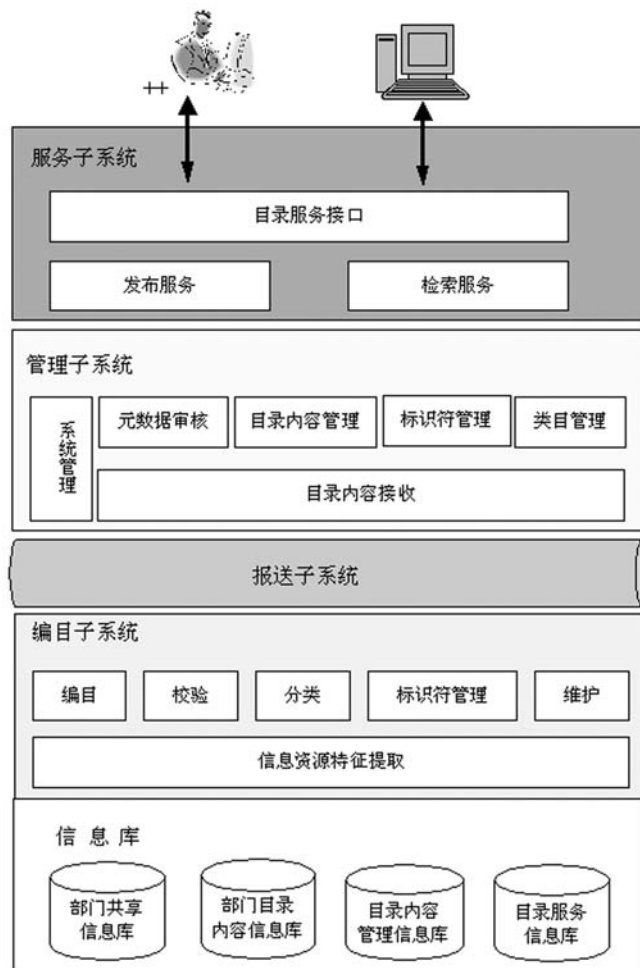


图3 目录内容服务系统

## 4.1 编目子系统

编目子系统为目录内容提供者提供目录内容的编辑服务。编目子系统由信息资源特征提取、编目、校验、分类、标识符管理等模块组成。

### (1) 信息资源特征提取

信息资源特征提取模块的主要任务是对本部门的共享信息资源内容进行分析,并对其进行特征合理识别和提取,形成信息资源的元数据。

### (2) 编目

编目模块是按统一的核心元数据标准,从部门共享信息库中抽取网页、数据库、电子文件等形态信息资源的元数据,形成规范的核心元数据,并保存到部门目录内容信息库。编目分为自动和手工两种方式。结构化数据(如数据库等)和半结构化数据的结构化部分(如网站中表格),采用自动编目方式;非结构化的电子文件,采用手工编目方式。在通常情况下,编目工作应该以自动编目为主要编目方式。

### (3) 校验

校验模块从语法的角度出发,检验核心元数据的合法性,保证格式正确、必选项完整。

### (4) 分类

分类模块按照统一的军事信息资源分类标准规定的分类要求,对元数据中的分类信息进行赋值。

### (5) 标识符管理

标识符管理模块按照统一的标识符编码方案的要求,对元数据中的标识符信息进行唯一标识符的赋码。

### (6) 维护

维护模块提供对核心元数据的人工修正,实现对冗余元数据的剔除,错误元数据的修改,以及必要数据的补充。

## 4.2 报送子系统

将编目子系统生成的、校验正确的目录内容以数据包的方式报送到目录中心,并保证数据传输的安全可靠。

## 4.3 管理子系统

管理子系统主要任务是对目录中心管辖的目录内容进行管理和维护。管理子系统由目录内容接收、元数据审核、目录内容管理、标识符管理、类

目管理和系统管理模块组成。

### (1) 目录内容接收

目录内容接收模块接收由报送子系统报送的部门目录内容,并保存到目录中心的目录内容管理信息库。

### (2) 元数据审核

元数据审核模块对提供者报送的核心元数据的语法和语意进行审核,以保证元数据的格式正确和语意合法合理;对元数据的编码进行审查,以保证元数据的正确来源;对元数据查重,以保证元数据的唯一性。其中自动审核是主要手段,人工审核为辅助手段。

### (3) 目录内容管理

目录内容管理模块主要是对目录中心的目录内容管理信息库进行维护管理,包括元数据的增、删、改,以及数据安全备份与恢复。

### (4) 标识符管理

标识符管理模块的主要任务是按照统一的标识符编码规则的要求,对提供者报送给目录中心的元数据,重新进行唯一标识符的赋码。

### (5) 类目管理

类目管理模块的主要任务是对目录结构进行维护,实现标准目录分类,以及用户个性化的目录结构扩展。

### (6) 系统管理

系统管理模块主要完成用户和权限管理、日志管理、系统配置管理等。

## 4.4 服务子系统

服务子系统的主要任务是完成目录内容的发布,提供目录内容的查询。服务子系统由发布服务、检索服务和目录服务接口模块组成。

### (1) 发布服务

将审核确定的元数据,根据军事信息资源分类标准,通过目录服务器,发布到目录内容服务信息库。发布服务模块的管理对象是目录服务器,它控制目录服务器的运行。并通过目录服务器的相关管理功能,可决定特定部分的元数据是否对外服务。

### (2) 检索服务

检索服务的主要任务是对服务请求的解析,提供有效的检索算法。

### (3) 目录服务接口

目录服务接口模块应符合统一的技术要求,实

现目录的对外访问接口,直接响应目录的服务请求。

用户的查询可以是使用者通过浏览器界面进行人工查询,也可以是其他应用系统直接通过目录服务协议进行查询。

## 5 关键技术

军事信息资源目录体系的建立需要相对应的技术支撑,从目录体系的建立以及目录内容服务系统的主要功能来看,建立目录体系的关键技术包括元数据采集技术、元数据存储技术、目录服务技术和目录应用技术。

### (1) 元数据采集技术

元数据采集技术包括元数据的自动采集技术和手工采集技术。自动采集技术一般和业务系统或者军事信息资源生产系统结合比较紧密。无论是元数据的自动采集还是手工采集,其基本核心包括两方面的内容:

一是对元数据内容标准的支持。不同的军事信息资源类型、不同的应用需求所需要的元数据内容是不同的。而且越是复杂的元数据内容标准,其内部的结构和相互关系就越复杂。因此,元数据采集应当支持对不同元数据内容标准的元数据进行采集,同时能够对采集的元数据进行数据完整性和逻辑一致性的检查。数据完整性主要指的是元数据内容标准中所规定的必选必填内容是否都已有值,逻辑一致性指元数据的实体和元数据元素的相互关系是否符合元数据内容的规定。

二是对元数据输出格式的支持。元数据采集完成后,必须首先输出再建立相应的存储。因此,元数据的输出必须采用成熟、主流的数据编码技术进行编码,方便元数据的输出和交换。目前,网络数据交换一般使用扩展标记语言 XML 进行编码,就参考文献(略)

### 作者联系方式

通信地址:北京市丰台区郑常庄 307 号院 R03 号

邮政编码:100039

联系电话:010-66820273-810

目前阶段而言,支持 XML 格式的元数据内容输出是必要的。

### (2) 元数据存储技术

元数据存储是目录体系的重要内容。元数据建库就是建立已经采集完毕的元数据的存储。目前,主流的信息存储是采用关系型数据库管理系统对信息进行存储管理,它具有工业化程度高、经济高效的特点。因此,军事信息资源元数据的存储需要尽量使用已有的关系型数据库进行存储。元数据是层次型数据,在存储到关系型数据库时,需要进行层次型到关系型的模型转换。如果直接针对元数据实体和元数据元素建立字段,无论对存储结构的稳定性和系统的效率来讲都是不可接受的。元数据的关系型存储的核心需要解决两个问题:一是存储的模式不会随元数据标准的变换而变化,需要在关系型数据库中建立元数据的数据字典描述元数据结构;二是要建立高效率的索引机制保证对元数据内容的有效检索。

### (3) 目录服务技术

目录服务技术是研究分布式环境下,信息资源元数据查询、提取的标准化处理技术。军事信息资源目录体系将按照统一的目录服务的技术接口标准,采用先进和成熟的技术来建立目录服务,为信息资源使用者发现、定位共享信息资源提供良好支持。

### (4) 目录应用技术

目录应用技术是向用户展现目录的技术。目录应用技术的核心是元数据的展现技术。目前,元数据一般采用 XML 进行编码,因此 XML 编码元数据的展现是目录应用技术需要重点考虑的问题。一般在 XML 元数据的展现方面有基于级连样式单(CSS)的技术,也有基于 DOM 和 SAX 的解析技术。我们需要基于此类技术,研究各种信息资源查询方式、元数据展示方式,已适应不同应用环境。

# 美军装备保障信息化的现状及发展趋势

徐宗昌 陈永龙 王军

**摘 要:** 装备保障信息化建设是美军在信息化时代装备建设及军队建设的一项重要内容。研究了美军进行装备保障信息化建设的目标,从保障理论、保障方式及保障信息系统等方面对其现状进行了分析,并指出装备保障信息化未来的发展趋势。

**关键词:** 装备保障信息化; 目标; 现状; 发展趋势; 一体化

在信息化战争初见端倪、信息化装备初显威力的时候,美军就领先世界各国一步,开始推行信息化发展战略,从理论发展到技术实践、从作战思想转变到实战检验、从武器装备更新到部队转型,无不让世界各国感到信息时代的强烈气息。早在 20 世纪 80 年代中期,美国国防部就开始推行 CALS 战略,从而拉开了装备保障信息化建设的帷幕<sup>[1]</sup>。

## 1 美军装备保障信息化的目标

美军认为装备保障信息化建设是一个是随着信息化战争需求的牵引和信息技术发展的推动,不断由低级向高级递进的长远发展战略,必须有明确的目标,为此,从国防部到各军兵种,美军制定出台了大量政策文件,其中典型的有《2003 年维修政策、计划和资源手册》、《美国国防部转型计划指南》、《2010 联合作战设想》、《军事术语词典》及各军种字典。这些文件将美军装备保障信息化的总体目标表述为:装备保障是战斗成功的核心因素之一,因而必须完全适应当前信息作战和未来信息化战争的特点,广泛应用最先进的理论、技术和设备、设施,并与战场环境、信息化部队及信息化装备等保障要素相适应,实现装备保障管理与指挥的信息化和装备保障手段的信息化。

## 2 美军装备保障信息化的现状

### 2.1 装备保障理论方面

#### 2.1.1 发挥信息优势,强调装备保障的精确化和实时化

伊拉克战争中,美军装备保障信息优势非常突

出:一是实现了装备保障全球化,依托“全球作战保障系统”,详细而精确地筹划和运用各种保障资源和力量。该系统能够对从伊拉克战场到分布全球的军事基地实施全程实时监测,并根据战场动态形势实施指挥和控制人员流、装备流和物资流的接收、分发和调换,从而为战略、战役、战术各个层次的军事行动提供相关保障信息<sup>[2]</sup>。二是实现了装备保障支援的实时化。在实际作战中,保障人员借助先进数字化通信网络,向远在千里之外的专家请求支援,在专家的实时指导下实现远程维修。必要时,五角大楼的维修专家也可通过先进的无线微波数字通信网直接对前方士兵进行维修指导,从而大大提高了战时装备的修复率。

#### 2.1.2 注重平战结合,随时提供强有力的保障

美军认为占据战争主动权的重要因素之一就是平战结合、超前预置。当前,美军实行三级战备制度,其中非战时的装备保障资源必须保证 80% 的有效率,以确保其装备保障的绝对实力。如为了保持装备的战备完好性,及解决因日常训练、演习和自然损耗所导致的战备完好性下降问题,陆军在 2003 财年支出 4.15 亿美元,其中超过半数以上用于常规武器装备保障资源的储备。国防部根据战略形势,分析地区特点,在全球范围内建立军事基地,在不同的基地储备相应保障资源,作为支持其全球战略的有力支撑点,一旦爆发战事,这些基地可立即投入使用,作为装备保障的基地,就近支援战场需要。

#### 2.1.3 实行全民动员,有效支持战时装备保障

目前,美国实行国家战争动员制度,这种全民动员有三种方式:广泛动员民用装备、广泛动员工业力量和广泛动员技术人员。根据需要,国家还可

以动用战略储备购买第三国的资源。伊拉克战争打响前,美军除紧急动员了大量包括快速海运船、海上预置船、浮动预置船等海军预备役船只外,还征用了大量民用商船和租借其他国家的商船和军用补充船。在本土陆地运输方面,美陆军军交管理局、铁路和汽车运输部门,协助完成作战装备和物资的装载运输。在科威特,美军租借、利用了大量当地的运输力量。此外,五角大楼还紧急征用和租用了部分商业卫星和民用信息网络,用以弥补信息传输能力不足。有资料显示,目前美军从事维修人员约68.1万人,已占美军总人数的23%左右<sup>[3]</sup>。

#### 2.1.4 运用战场抢修理论,持续提高战场抢修效率

美军战场抢修理论研究起步较早,早在1982年,国防部就制定并颁布了《战场损伤评估与修复纲要》,用于对各军种的战场损伤评估与修复工作进行集中指导,同时还制定和编写了种类齐全、可操作性强的相关条令和技术手册,建立起较为完善的战场抢修理论体系,并研制了一整套先进的战场抢修装备及专用工具箱,因此,美军的战场抢修能力和水平远远领先于世界各国。所有这些努力,在美军历次战争中得到了有效的回报。在伊拉克战争中,尽管大量装备受到伊军的重创及高温、沙尘等恶劣环境的影响,但受损装备凡是能修复的,都在24小时内完成修复,最快的甚至只有几十分钟。由于抢修及时,美军武器装备保持了很高的战备完好率,有力地支持了部队的作战行动。

## 2.2 装备保障方式方面

### 2.2.1 联合保障

当前,美军已经开展的联合保障主要有两种模式:一种由军队最高指挥机构直辖的保障力量对参战的各军种提供所需要的一切保障;另一种则由联勤机构或国防部指定的军种负责属于全军通用的保障任务,军种专用的保障任务由各军种自行负责。为了在战争中实现部队联合保障,美军通常在战区设立专门的保障指挥机构,其成员由来自各军种的代表组成。美军条令规定,战区陆军司令部还是战区保障指挥与控制及基础设施的唯一提供者,因此,战区保障副司令通常由战区陆军司令或副司令担任。目前,美军独立于各军种之外的联合机构——国防后勤局和运输司令部的发展也十分迅速。国防后勤局负责全军200多万种通用物资的采购与供

应。运输司令部则把原属各军种的军交运输管理司令部、军事海运司令部和军事空运司令部及其运输力量统一起来进行指挥。

### 2.2.2 精确保障

在《联合设想2020》中,美军明确地提出了精确保障(Precision Logistics,也有翻译为“精确后勤”的)的理论与要求:以信息的获取和利用作为保障的核心要素,以完美的保障信息自动化为基础,精细而准确地筹划、建设和运用装备保障力量,在准确的时间、准确的地点为部队作战提供准确数量和高质量的装备保障,最大限度地节约保障资源。准确掌握部队的保障需求是前提,为此,美军在全球范围内建立了完善的自动化信息网络;全资可视化能力是发展重点,目前美军各军种、各部门都在国防部相关标准和规范的要求下,按照统一的标准和形式,发展各自的资产可视化系统,这些子系统最终将由国防部联合成一个综合系统,以更好地满足完成装备保障任务的需要;主动配送是发展核心,美军将传统的被动补给型保障转变为高效的主动配送型保障,将前沿存在型保障转变为投送型保障。

### 2.2.3 多元化保障

美军装备保障越来越明显的体现出多元化的特征。① 现役部队仍然是实施装备维修保障的核心力量。由于现役部队是受过严格的军事训练、配备性能优越的设备、拥有充足的保障资源,一般能够确保装备保障任务的完成。② 预备役部队是战时装备保障力量的重要组成。美军为了使现役部队更加精干,以低投入、高效率弥补现役部队保障力量的不足,使用了大量预备役部队保障力量。目前,美军第一类预备役人员总数约为70万,其中从事装备保障的约占27%,达到19万人。③ 合同商是装备保障力量的有效补充。现代武器装备的技术含量不断提高,战场环境的日益复杂化,单纯地依靠部队力量进行装备保障已经不可能完成,美军主张通过大力鼓励利用合同商完成保障工作。

### 2.2.4 交互式电子技术手册

交互式电子技术手册(IETM)是美军装备全寿命信息管理策略中一项重要的信息化保障技术,其基本原理是构建一体化、数字化的集成数据环境,形成可重复利用的信息资源,降低保障成本、



提高保障效率。按美国防部的规划, IETM 将内容以数字形式储存, 实现了技术资料和使用手册的数字化, 并赋予其强大的交互功能, 通过计算机和网络, 借助电子显示系统, 将保障人员或系统操作人员所需的特定信息(包括文档、声音、影像、图片等), 精确而直观地展现在使用人员面前, 目的是利用信息技术, 改变传统纸张型技术手册在制作、使用、保管、储存等方面的不便, 实现了技术手册的智能化, 加速保障人员执行任务的速度, 提高装备的可靠性和维修性, 提升装备保障的效率, 降低寿命周期费用<sup>[4]</sup>。

## 2.3 装备保障信息系统方面

### 2.3.1 以C<sup>4</sup>ISR系统为核心推进装备保障信息化进程

美军目前拥有一个极其庞大的、覆盖全球的C<sup>4</sup>ISR系统, 其技术、设备、规模与能力都是世界最先进的, 但由于各军种在建设自己的C<sup>4</sup>ISR系统时对其他军种系统之间的互连、互通性考虑不够, 更未考虑与联合作战相应系统的接口问题, 因而造成了系统之间信息交换的困难。虽然在C<sup>4</sup>ISR持续发展的过程中, 这个问题得到了不断改进, 但至今尚未被彻底解决。按照“勇士”C<sup>4</sup>ISR计划, 美军联合总部、陆军、空军、海军和陆战队所属系统将分别从14、26、38、34、21个集成为一个, 再通过全面实现互连、互通、互操作后, 最终集成为一体。此外, 美军还确定国防部“全球信息栅格(GIG)”计划的定义、构想、政策和要求, 将保密及非保密计算机网络连接成全球性信息网, 目的在于为决策层和陆、海、空参战人员实时提供数据。GIG计划开始进入实施阶段。

### 2.3.2 全资可视化信息管理系统广泛应用

“全资可视”(Total Asset Visibility)是美军装备保障从工业时代转向信息时代的核心概念, 也是美军后勤保障效率得以大幅提高的核心因素, 当前“全资可视”的概念正在向装备保障领域扩展, 并得到了越来越广的应用。“全资可视”的核心是将自动识别技术、全球运输网络、联合资源信息库和决策支持系统综合在一起, 联合部队指挥官可以不间断地掌握全部资源的动态情况, 全程跟踪人员流、装备流和物资流信息, 指挥和控制其接收、分发和调换, 为有关管理与保障人员及时提供物资供

应线上资源的位置、运动和状态的准确信息, 以确定部队、人员、设备和供应品的状况, 同时还报告资源的生产、修理、部署、需求和库存量的状况, 从而大大提高了资源保障效率<sup>[5]</sup>。目前, 美军将全资可视化技术及相关系统建设作为实现《联合设想2020》的一种重要技术途径。

### 2.3.3 几个典型的信息管理系统

1) AN/MYQ-4A 作战后勤保障控制系统。已经装备陆军旅以上各级指挥和保障梯队, 用以代替执行军以上作战后勤保障控制系统的一些功能。该系统具有情报采集、传递及处理, 军种专用物质保障、技术保障的控制管理及军事运输保障等功能。

2) 直升机装备机械状态诊断与使用综合管理系统<sup>[6]</sup>。该系统在直升机飞行过程中收集飞机系统状态信息, 在飞行结束时, 将这些数据传送给地面计算机系统作处理、分析并据此确定应采取的维修活动。

3) 维修要求系统。该系统是专门为海军设计开发的一种全新的舰艇维修和可用性规划工具系统, 已于2000年开始在水面舰艇上试用。

## 3 美军装备保障信息化的发展趋势

### 3.1 电子信息系统继续向综合化方向发展, 成为武器装备体系发展的关键

#### 3.1.1 用体系结构框架指导武器装备一体化建设

美国国防部在《C<sup>4</sup>ISR体系结构框架》(2.0版)的基础上制定了《国防部体系结构框架》(1.0版), 并要求2003年12月1日之后开发或批准的所有体系结构必须遵照该标准, 此前开发的体系结构必须加以修改。将体系结构方法从C<sup>4</sup>ISR系统扩展到所有与信息系统相关的领域, 从根本上保证与电子信息系统有关的建设一体化。《国防体系结构框架》(1.0版)确定了以应用为基础的体系结构内容, 并支持国防部需求生产系统(RGS)、规划/计划/预算系统(PPBS)和采办管理系统(AMS)<sup>[7]</sup>。实践表明, 先进的体系结构框架是构建一体化武器装备体系的根本保证。

#### 3.1.2 “全球信息栅格”将继续快速发展

全球信息栅格带宽扩展(GIG-BE)计划已使

部分节点具备初始作战能力；转型通信卫星进入概念验证阶段，预计第一颗将于 2011 年发射升空；新型联合无线电系统（JTRS）取得实质性进展；决定开发新一代指控系统，并最终取代全球指控系统；互联网转型工作取得突破性进展。IPv6 成功进行了两次阶段测试，标志着美 IPv6 建设取得突破性进展。此外，各军种也正在大力开展信息基础设施建设，继美海军提出“部队网”和空军提出“星座网”概念后，陆军于 2004 年提出建设“陆战网”，三个网络都将作为 GIG 的重要组成部分。

### 3.1.3 着重解决数据链的融合问题

为了实现作战平台与各种传感器信息的实时共享和高效利用，以及对武器系统的实时控制，美军在作战平台上普遍加装数据链，并积极开发可纳入 GIG 的武器控制用数据链，使武器能够利用其他传感器系统获得的信息，提高打击精度和实时打击能力。正在研制的“联合增程透明多平台网关设备组件”（JTEP）系统，将使装备了 Link-16 和态势感知数据链的飞机实现与报告中心之间的自动通信。计划今后 10 年内在包括 F-15、F-22 战斗机、F-35 “联合攻击战斗机”、无人驾驶飞机和 B-52 轰炸机等 4000 个作战平台上，装备升级后的 Link-16。

## 3.2 电子战装备向一体化发展，计算机网络战装备趋于实用化

### 3.2.1 电子战装备的一体化

美军将实现不同功能、不同类型的电子战系统以及电子战系统与火控系统、通信系统等进行系统集成。美军还将飞机雷达报警系统、导弹计算机、射频干扰系统和拖曳式干扰系统完全综合到一个系统中，试验了“综合防御电子对抗系统”。正在研制的“狼群”分布式干扰系统，将众多小型干扰机部署在干扰目标周围 100 米以内，依靠网络联在一起自动工作。另外，还积极推动新概念电子战装备的发展，预计在未来 5 年内高功率微波武器技术可投入使用，未来 8 到 10 年，100 千瓦的高功率固体激光器将投入使用。

### 3.2.2 规划计算机网络战的未来任务

提出到 2020 年，将具备对所需攻击网络的侦察能力、对网络攻击效能的评估和再攻击能力，以及灵活的计算机网络攻击能力和在战术级使用计算

机网络攻击的能力。美军还在研制各种计算机病毒、芯片武器、计算机穿透技术、通信干扰等手段和武器，开发无线和有线远距离注入计算机病毒武器，能找出敌方计算机或电话系统漏洞的技术，影响决策人员正确决策的“攻心武器”，以及先进的精确网络攻击武器，以实施 100% 的精确打击<sup>[8]</sup>。通过训练、演习等手段，提高对敌网络的侦察能力和攻击能力，以及对空间系统的打击能力。

### 3.2.3 注重信息安全

美军的全球信息栅格建设，从初期就将网络安全作为建设的重要内容，采用了多层配置、深层防护的综合信息防御策略。美军还特别强调提高对空间系统的信息对抗能力，保证空间信息系统的安全，提高其可用性和生存能力。

## 3.3 保障装备及保障理论、技术和体制出现新变化

### 3.3.1 保障装备向多功能、通用化、网络化、智能化的方向发展

为节省设计、生产、维修的时间和费用，美军将研制生产多功能、通用化的保障装备。如美空军正在实施的“多功能飞机地面保障系统（MASS）”计划，F-117A 隐身战斗轰炸机也采用了很多与其他飞机通用的保障系统。为满足联合作战需要，保障装备将向网络化发展。目前主要是大力发展远程保障系统和提出“以网络为中心的维修”概念，最大程度地利用互联网和军用通信网络，使维修机构和维修人员能够通过安全的网络化设施解决装备保障问题。为提高保障装备的智能化水平，利用人工智能技术开发先进的故障诊断设备和专家系统。

### 3.3.2 保障理论、技术和体制的新变革

一是保障理论不断创新。美军提出“以网络为中心的维修”和“基于状态的维修”等创新性理论，目前正在美军“联合攻击战斗机故障预兆状态管理项目”、“陆军诊断改进计划”、“海军综合状态评估系统”等战略性维修项目中尝试。二是开发和应用新的保障技术。不断将计算机技术、人工智能技术以及网络技术等现代高新技术应用于装备保障领域，形成了以“快速制造技术”等为代表的现代保障技术，极大地提高了保障效能。三是优化保障

体制。重点是简化装备保障级别，消除一些冗余设置；简化物资供应环节，优化供应体系，显著提高物资供应效率。

型阶段，并呈现出加速发展的趋势，信息化、一体化成为武器装备发展的总趋势，与之相应的装备保障信息化建设也成为美军研究和建设的重点。虽然在装备保障理论、保障方式及信息系统等方面走在世界的前列，但为谋求军事上的绝对优势，美军仍然在装备保障信息化的软、硬件上加强建设。

## 4 结束语

美军的武器装备发展正处于机械化向信息化转

### 参考文献

- [1] 徐宗昌.保障性工程[M].北京:兵器工业出版社, 2002
- [2] 总装备部科技信息研究中心.美军的“全球作战保障系统”[J].装备维修保障动态, 2005, 10:5-6
- [3] 总装备部科技信息研究中心.美军装备维修保障概述[J].装备维修保障动态, 2005, 17:1-2
- [4] 美国国防部.DoD D5000.1.“The Defense Acquisition system”[R].2000
- [5] 王铁宁.装备保障信息系统工程[M].北京:装甲兵工程学院, 2003
- [6] 总装备部综合计划部.信息化战争装备维修保障[M].北京:国防工业出版社, 2007
- [7] 军事科学资料中心.美军防务采办改革的发展动向[J].www.defence.org.cn.aspnet/vip-usa
- [8] Robert D.Paulus. A Full Partner'-Logistics and the Joint Force[J]. Army logistician, 2003, 35 (4)

### 作者联系方式

通信地址: 北京市丰台区杜家坎 21 号装甲兵工程学院技术保障工程系

邮政编码: 100072

联系电话: 010-66719453

# 军事信息基础设施建设研究

许晓波

**摘 要：**本文重点讨论了未来战争军事需求，分析参考了外军军事信息基础设施体系结构建构方法，对我军的信息基础设施体系结构建构方法进行了讨论，提出了军事信息基础设施建设的成功要素和发展建议。

**关键词：**信息基础设施；体系结构建构方法；C<sup>4</sup>ISR

## 1 引言

军事信息基础设施是军队信息化建设的一个重要组成部分，也是军队信息化建设的基础。信息基础设施本身就是一个多领域的涉及面较宽泛的概念，它包含了通信、网络、信息处理、信息安全保密、管理（信息分发管理、系统和网络管理等）甚至支持服务等方面领域。也是将来建设军事信息栅格、信息平台与武器平台无缝连接和实现 C<sup>4</sup>ISR 的基础支撑。

## 2 未来战争军事需求分析

自海湾战争以后，一场比一场信息化程度更高的战争陆续搬上了舞台。反复诠释着信息制胜的理念。谁掌握了信息优势，谁就有更大把握赢得战争。世界各国在军事建设中都加快了信息化建设的步伐，夺取信息优势成为各国军队竞相追求的目标。美军提出战争将从“以平台为中心”向“以网络为中心”转变，要求发展强大的计算机信息网络，以便将分布在广阔区域内的各种探测系统、指挥控制系统和武器系统组成统一高效的大系统，共享战场资源，相互交换信息，制定作战计划。美国防部提出了 C<sup>4</sup>ISR 体系结构框架，并提出了“全球信息栅格”（GIG）的概念，其实质就是建设遍布全球、高度网络化的国防信息基础设施，使其成为信息化武器装备体系的基础，改善作战决策能力，克服各军兵种的信息系统难以互连、互通、互操作的弊端，消除信息系统“烟囱林立”和“信息孤岛”现象。

未来作战将是各军兵种的联合作战，一体化的

C<sup>4</sup>ISR 是基础，国防信息基础设施是重要保障。俄罗斯军事专家认为，未来战争中将出现网络战、指挥控制战、导航战等形式的信息战。这就要求建设攻防兼备的信息战装备，不仅要大力建设对各类电子系统或网络有摧毁、破坏作用的武器装备，而且要加速建设确保信息安全的各种防护系统和快速恢复系统，并要不断提高各种信息系统的安全性和抗毁性。从海湾战争、科索沃战争到伊拉克战争，无不表明了控制信息优势对战争进程的决定作用。世界各国都在运用信息技术对现有武器装备进行改造，同时加紧研制新型信息化武器装备。这的信息化建设顶层设计也有一定的指导意义。

军事信息基础设施必须满足作战需求。注重顶层设计是军队信息化建设最成功的经验之一，它是作战需求的产物。如果忽视了作战需求，仍各自为政进行建设，必然出现“烟囱林立”，重复建设的败笔之作。需求牵引一是要以信息为主导，运用“三军一体、网络融合、综合应用”的新理念，替代“按地域建设、按业务组网、按军种使用”的传统模式；二是互连互通，坚持统一规划、统一组织、统一标准，实现信息资源共享，遏制“烟囱”蔓延；三是简捷实用，适应电话、计算机和图像“三网融合”的发展趋势，切忌只顾短期效益，忽视长远规划。所以应从全军信息建设顶层设计考虑，研究军事信息基础设施的体系结构建构方法。

## 3 军事信息基础设施体系结构建构方法讨论

美军在海湾战争后发现，要想获得绝对优势的战场空间态势感知，只有一体化的、互操作的、高效的、基于标准的 C<sup>4</sup>ISR 能力才能满足任务需要。

基于这一认识，美国防部改变了原有的孤立式开发方针，转而采用开放式系统工程方法，制定了《信息管理技术体系结构框架》《联合技术体系结构》《国防部体系结构框架》《C4ISR 体系结构框架》等一系列文件作为美军发展综合电子信息系统的最主要的指导性文件。提供了建立和集成体系结构的六步方法：一是确定体系结构的使用意图；二是确定体系结构的范围；三是确定要抓住的特点；四是确定要建立的视图和产品；五是建立必不可少的产

品；六是有目的地使用体系结构。  
对于我军军事信息基础设施这样一个涉及面宽、多领域的综合信息系统，为了保证建立的体系结构能够满足战争发展需求，又具有技术可实现性，就必须采用多视角切入的开放式系统工程的方法，进行自顶向下的设计，然后对构筑的体系进行综合分析评价，并及时采用反馈分析方法自下而上进行调整完善。参照上述构建方法，在这里提出一种方法进行讨论。构建步骤如图 1。

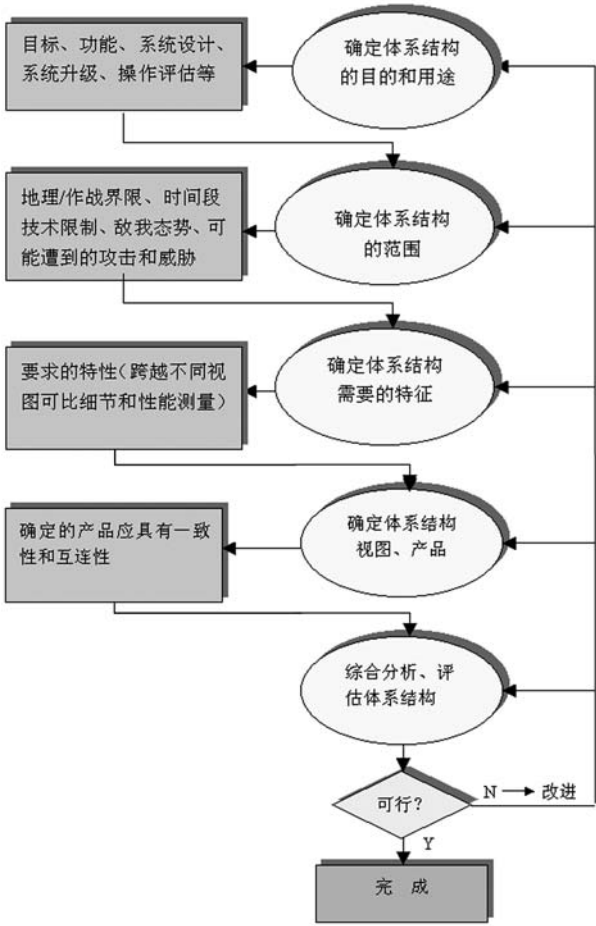


图 1 体系结构构建步骤

- 1) 从战场环境应用和作战任务需求出发，确定信息基础设施体系结构的目的是和用途。  
要针对特定的应用目的和用途来建立信息基础设施体系结构，才能提高效率和物尽其用。目的和用途可以是应完成的功能、由此而进行的系统设计、系统升级、用户培训、互操作评估等等。
- 2) 确定信息基础设施体系结构的范围、背景、环境和假定。  
在确定目的和用途以后，需要确定信息基础设施体系结构的范围（如行动、组织、机构、时间

- 等）、详细程度、工作内容、作战想定、敌我态势、系统可能遭受的攻击和威胁、地理范围、经济状况、技术可获取性、计划管理因素影响、资源与经验可获得性等。
- 3) 确定信息基础设施体系结构需要的特征。  
在确定信息基础设施体系结构的范围、背景和环境后，需要确定信息基础设施体系结构的特征。为实现信息基础设施体系结构的目的是和用途，信息基础设施体系结构应当具有合适的特征，以保证任务的完成和资源的充分利用。

4) 确定信息基础设施体系结构的视图、基本产品和辅助产品。

在确定信息基础设施体系结构的特征后, 需要确定为具备这些特征所需要的信息基础设施体系结构视图、基本产品和辅助产品。其中基本产品是必备的, 辅助产品则是可选的。并要求这些产品具有一致性和互连性。

5) 综合分析、评估能否满足上述目的和用途的信息基础设施体系结构。

6) 对综合分析及评估结果对体系结构进行调整和改进。

以上六个步骤, 从预定信息基础设施体系结构的目的和用途开始, 到对构建体系结构的综合分析评估, 最终达到预期的目的, 是一个循序渐进的多重循环过程。

## 4 我军信息基础设施建设成功的要素

### 4.1 从战争需求的角度全面审视信息基础设施结构

军事信息基础设施是军队信息化建设的基础, 也是信息系统架构的具体实现, 所以必须从需求的角度出发, 建立和完善三军信息系统间, 信息系统和其他系统平台间的相互联系和关系, 使建立的信息系统能够在真正意义上实现三军的互连、互通以及与其他系统平台间的互操作。

信息基础设施不仅涉及到系统本身, 还涉及到构成系统的各种基本硬件产品、软件(包括统一的规范、标准等)、组织结构甚至包括人力资源等, 是一个复杂的、涉及面宽的系统工程。各级领导层的共识和充分重视是成功的基本保障。

### 4.2 重视规划, 不断完善信息基础设施

信息基础设施涉及的技术领域宽, 构成的基本产品多样化, 这些问题增加了我军信息基础设施建设的难度。信息基础设施的建设过程必须与当前技术的发展现状和目前的装备现状结合同步进行, 因此必然是一个循序渐进、不断完善的过程。

制定科学、合理而又切实可行的建设规划, 自顶而下组织实施建设。要做好建设规划, 必须全面评估信息基础设施的现状, 了解当前及今后军事技术发展趋势以及战争转型对信息设施的需求, 在此

基础上设定建设目标, 规划适当技术体系架构。从未来战争需求—任务层面—信息基础设施的宏观角度把握信息基础设施的架构、接口和网络系统。科研单位、工业部门在这方面要为军队的信息化建设当好参谋, 服好务。

### 4.3 关注架构, 以发展的眼光分层设计支持快速开发

在当今科学技术迅猛发展的时期, 战争形态的变化与科技发展密切相关。军队必须更快捷地响应和把握不断变化的战争形态, 才能把握战争、赢得战争。为此我军的信息化建设也要随着战争需求发展和技术的发展而滚动发展。那么在架构设计时就应注意其灵活性、易构性和重建性。

信息基础设施的架构包括功能架构、系统架构、数据架构、基本流程等。在架构设计和实施过程中, 要特别重视基本流程、网络和系统间的衔接, 以简化的流程和架构设计支持快速开发, 适应发展需要。

分层结构设计(表示层、逻辑层、数据访问层)能够提高系统架构的灵活性; 功能组件的标准化封装能够提高软件的复用度; 数据集中能够保证数据的一致性和准确性, 而标准化设计和统一选型能够降低成本和复杂性。

在架构设计中, 还必须考虑可靠性、使用性、维修性以及可扩展性。注意变化管理和问题管理, 明确相关的测量指标, 结合需求和技术可能, 从纵向结构和横向专业(包括业务平台)的角度审视架构、流程、系统和信息流, 仔细验证架构的合理性。

## 5 发展建议

要搞好我军的信息化建设, 最根本的一条是科学认识信息化建设的规律, 扎扎实实地解决信息化建设的最基本问题, 这是推进军队信息化建设的全面协调和可持续发展的关键。

### 5.1 搞好顶层设计——搭建通用平台

信息基础设施是构建三军“通用平台”的基石。信息基础设施包括信息传输平台和信息处理平台以及管理平台等部分, 其特征: 一是通用性, 能够为军队多数信息系统共享共用, 有统一的技术标

准和运用规则；二是稳定性，能够长期运行，各种软件版本符合标准化要求；三是独立性，关键信息设施的最小集合能够自成一体、独立遂行保障与服务。

搞好顶层设计，制订统一标准，是抓好信息基础设施建设的保障。只有明确了要达到的目标、实现的功能、建设的思路和方法以及必须遵循的统一技术规范和技术体制，信息化建设才能有章可循，才不会出现新的“烟囱”式系统。这也是信息化建设和机械化建设的重要区别之一。

## 5.2 加速装备改造——挑战物理极限

信息技术是武器装备升级换代的直接动力。以微电子、通信和计算机为主体的信息技术，在嵌入武器装备之后，其精确度相当高，而外型趋于小型化，功效趋于智能化，携弹量增加，杀伤力与大型武器装备相当，且不受天候和战场条件制约，可对锁定目标实施全天候昼夜精确打击。此外，利用信息技术，多种类的作战平台有机联网，集指挥控制、情报侦察、预警探测、精确打击和战场管理于一体，以作战平台的网络化来提高一体化联合作战能力。

正确选择武器装备信息化改造的道路。一是对现役武器装备进行信息化改造，使其具备原先不曾有的信息探测、传输、处理、控制和对抗等功能，从而实现装备性能和作战效能的质变。二是研制新型信息化武器装备，用全新的设计思想和顶尖技术研发新装备，强化其探测、识别、打击、机动、定位和隐身等综合功能，增加武器库中的“新种群”。从 20 世纪 90 年代末开始，西方发达国家凭借其强大的经济和科技实力，把发展新型信息化武器装备作为军队转型的重要内容。处于机械化的发展中国家，在重视发展新型信息化武器装备的同时，依然坚持把武器装备信息化改造视为提高战斗力的有效途径。

武器装备信息化改造必须提速。从机械化向信息化转型，对于发展中国家来说，重点是尽快改变武器装备的半机械化、机械化并存的落后局面。信

参考文献（略）

作者联系方式

通信地址：成都 810 信箱 15 分箱中国电子科技集团公司第三十研究所

邮政编码：610041

联系电话：028—85169635

息化是从机械化基础上起步的，即便是发达国家，也无法跨越机械化而直接进入信息化，因此，必须十分重视利用先进的信息技术对机械化武器装备实施信息化改造。例如，俄军 A-50 预警机建于 20 世纪 70 年代，由于俄军利用先进的电子技术和装备对其进行不间断改造，目前该飞机除了外壳改动不大外，里面的航空电子设备已面目全非，至今仍属于世界领先的预警装备。

## 5.3 开发信息资源——减少信息“孤岛”

信息资源开发是信息化建设的中心任务。军事信息资源开发利用，就是运用现代信息技术整合使用信息内容及相关人力物力财力资源。一位军事家指出：“军事信息资源缺乏，就如同枪炮没有弹药；作战指挥离开了信息，就失去了决策的依据；武器装备没有可靠的信息保障，精确打击就不能实现”。可以说，没有信息资源战争机器就无法运转。目前，某些西方发达国家军队的信息资源开发利用已处于世界领先地位，仅地理信息系统就具备了获取全球除两极之外 90% 的数字信息的能力。

统一标准是开发信息资源的根本保证。没有统一标准就不能实现互连互通和资源共享。首先要建立标准化体系，统一信息分类、信息编码、数据格式，规范信息的生产、存储和应用过程。其次要推进标准通用化，便于引进吸收先进技术，加强国际国内交流合作。

## 6 结束语

世界新军事变革的加速发展，即给我们带来了新的机遇，也给我们提出了新的挑战。能否适应这种新的发展趋势，把我军的信息化建设搞上去，直接关系到我国在 21 世纪能否占据更加有利的国际战略地位，关系到我们能否打赢未来可能发生的高技术局部战争。所以我们一定要抓住这个机遇，为我军的信息化建设架好桥、铺好路。

# 美军联合通信与指挥控制系统建设

杨茜 李申 张灿

**摘要：**作为未来联合作战能力的转型基础，联合指挥控制能力是网络中心战的关键赋能器，也是实现信息和决策优势的重要保障。本文在分析美军现有联合通信与指控系统能力的基础上，对系统的发展脉络进行了梳理，并总结了美军实现联合通信与指控系统能力的途径。

**关键词：**美军；联合通信；联合指挥控制

## 1 美军现有联合通信与指控系统能力分析

美军现有联合系统只重视关键信息的交换，并未强调各联合部队之间扁平的信息流。烟囱式的指控系统不利于联合互操作能力的发挥，信息交换不够快速和无缝。影响了战时和平时对作战人员、政策制定者以及支持机构进行有力支持的能力。

### 1.1 作战准备能力

联合通信与指控系统可为指挥官提供全面的规划报告以便更准确、及时评估联合部队如下方面的能力：准时在指定地点执行指定任务、认识到作战中的不足、评估任务风险、在关键行动中领导所有部队、接收部队部署信息以及分析作战趋势等。美军要求系统提供全面的可视化评估以增强部队作战准备的准确性和有效性，但美军现有联合通信与指控系统在为部队提供有效作战准备评估方面尚存在一定的不足。

### 1.2 联合情报分析能力

联合通信与指控系统可提供情报分析能力，将生成的情报和信息综合进国家数据库；将高级联合战场情报准备、确定目标和情报、监视、侦察管理能力集成进一个通用作战图像，为指挥官、联合部队指挥官提供关键情报支持。不足之处是美军现有联合通信与指控系统有时不能快速对战区情报、战术图像以及其他相关情报进行集成。

### 1.3 态势感知能力

联合通信与指控系统可为指挥官提供对战场空间的监视能力以实现决策优势，同时提供准确、完整、及时、相关的战场信息，这些信息具体包括：蓝军和红军跟踪、态势数据（图像等）、定位信息、环境数据、用户告警以及过滤或拉取与当前工作/任务有关的数据。联合通信与指控系统还应提供能够支持决策制定的信息，以缩短决策周期、支持有效计划同时实现快速决策作战。美军正在加强通过可共享的态势感知对部队进行指挥控制的能力。

### 1.4 联合业务能力

联合通信与指挥控制系统可支持所有所需节点，高级联合业务能力还应能够具有音频、视频、视讯会议、白板、聊天以及应用共享功能。美军认为其现有联合通信与指控系统在提供支持横、纵向指挥控制信息交换的综合协作能力方面尚有欠缺。

### 1.5 安全能力

联合通信与指挥控制系统可实现不同保密级别信息从/到多个数据资源的“推送”/“拉取”，实现保密、及时、有效的信息检索和分发，进而为指挥官提供态势感知能力并缩短决策周期。美军正在大力解决现有联合通信与指控系统不能提供不同密级间的协同问题。

### 1.6 训练能力

联合通信与指挥控制系统可支持可定制的训练，通过在线访问来支持训练。美军联合通信与指



控系统正通过各种方式克服不足,提供综合、基于在线辅导的计算机桌面帮助工具及相关技术文件以满足操作人员、值勤人员及系统管理、维护和训练的需要。

## 1.7 办公室自动化能力

联合通信与指挥控制系统应能够翻译基于文本的文件/记录以支持战略和作战层的信息交换。美军现有联合通信与指控系统正寻求提供各种语言翻译能力的办法。

## 1.8 文电传输及信息保障能力

联合通信与指控系统必须能够提供保障可共享的 C<sup>4</sup>ISR 信息的能力,防止可能的网络威胁。系统还必须能够通过联合防护、探测及相应能力来保障系统在受到攻击后能够得以恢复。美军现有联合通信与指控系统尚不能提供完善的内置文电处理能力。有时只能将电子邮件、用户信息等业务集成入决策支持环境。

# 2 美军联合通信与指控系统的发展

美军针对其联合通信与指控系统存在的问题与不足,积极采取有效措施,大力推进系统发展,提升系统能力。

## 2.1 联合通信系统的发展

在联合通信系统方面,美军采取战略、战役、战术层齐头并进的发展思路,以构筑覆盖全面的一体化联合通信系统。

### 2.1.1 战略层推进“全球信息网格”建设,为实现 C<sup>4</sup>ISR 系统一体化奠定基础

20 世纪 90 年代初,针对海湾战争中各军种烟囱式的 C<sup>4</sup>I 系统互连互通能力差的弊端,美军提出了建设一体化 C<sup>4</sup>I 系统的发展战略,并于 1999 年 9 月提出建设全球信息网格(GIG)。目前,美军已完成 GIG 的顶层设计,进入系统全面建设阶段。美军将以转型通信体系结构作为 GIG 通信设施的主体,构建由地面、空中和空间三部分组成的一体化通信网络。地面通信主要是依照“GIG 一带宽扩展计划”建设的光纤网;空中通信采用具有变频和 IP

路由能力的联合战术无线电系统;空间通信则主要依赖于根据“转型通信卫星”计划建设的通信卫星星座。此外,天基系统和飞行器之间采用宽带激光通信连通,天基系统和地面之间采用激光通信或可编程无线电连通,此外,通过远程通信端口还能够提供卫星与地面、卫星之间、空中系统之间的连接。

### 2.1.2 战役层各军种建设各自的一体化网络,最终实现网络集成

美军各军种为了适应 GIG 的发展需求,都提出了各自的网络发展计划,将过去众多的网络集成为一体化网络,成为 GIG 体系的子网。为了实现各军种网络的一体化,美军于 2004 年明确了各军种子网建设应遵循的框架、标准以及联合体系结构。这些子网包括陆军的“陆战网”、空军的“星座网”和海军的“部队网”。

### 2.1.3 战术层着重发展数据链,实现“从传感器到发射器”的无缝连接

数据链作为实现作战平台之间、作战平台与信息系统之间信息实时传输的手段,可实现“从传感器到发射器”的无缝连接,是实施网络中心战的关键装备。为了克服 Link 16 只能进行视距通信的局限性,美军正实施 Link 16 增强型数据链和卫星战术数据链研发项目,并计划 2015 年前后用 Link 16 增强型取代现有数据链。同时,美国还通过融合 Link 16 和 Link 11 的功能和特点开发 Link 22 数据链。其次,由于现有数据链已无法满足传输文本、语音以及图像等大容量数据的需要,美军正在研制各种新型数据链。随着这些新型数据链的投入使用,美军联合作战效能必将大大增强。

## 2.2 联合指挥控制系统的发展

在联合指挥控制系统方面,美军着力实施从“全球指挥控制系统”向“联合指挥控制系统”过渡,同时加强了各军种指挥控制系统的互操作能力建设。

### 2.2.1 “全球指挥控制系统”向“联合指挥控制系统”过渡

全球指挥控制系统(GCCS)是美军进行联合作战和多国联合军事行动的战略指挥控制系统,于

1996年7月开始服役。经过多年的使用和改进, GCCS 已发展为一个适用于不同军种和作战地域的指挥控制系统, 能够支持各级指挥层的所有应用。利用该系统, 美军只需3分钟便可使全球战略部队进入战备状态。但是 GCCS 缺乏足够的灵活性和信息共享/协同能力, 不能满足网络中心战的要求。为此, 美军决定从2006年开始部署联合指挥控制系统(JC<sup>2</sup>), 逐步取代 GCCS。联合指挥控制系统的所有服务和功能都将以全球信息网格为基础, 具有高效决策、认知共享、灵活同步、分步式指挥控制、高效的组织结构、全面集成、可共享的高质量信息、强大的组网能力, 以及连续的、一体化的网络中心性能等显著特性。预计2010年左右, 联合指挥控制系统将具备完全作战能力, 2015年后, 美军所有的军事行动都将通过联合指挥控制系统来指挥实施。

### 2.2.2 陆军作战指挥系统实现互操作

美军的战术指挥控制系统主要由陆、海、空三军战术指挥控制系统构成。本文主要分析陆军作战指挥控制系统(ABCS)。目前, ABCS 已经建成为以国家信息基础设施为依托, 以战术级战场信息控制系统为基础, 以战役、战略级指挥控制系统为支撑, 以单兵指挥控制系统为末端的战术指挥控制体系。ABCS 由12个系统组成: 陆军全球指挥控制系统、21世纪部队旅和旅以下作战指挥系统、高级野战炮兵战术数据系统、防空与防导规划控制系统、全信源分析系统、作战指挥维持保障系统、战斗地形信息系统、战术空域综合系统、机动控制系统、综合气象系统、综合系统控制和 ABCS 信息业务服务器。

## 3 美军实现联合通信与指控系统能力的途径

纵观美军联合通信与指控系统建设历程, 可分析得出美军在实现联合通信与指控系统能力过程中采取了以下方法与途径。

### 3.1 建立专门的联合指挥与控制机构

为加强联合作战, 提升联合通信与指控系统能力, 美军调整组织机构, 将现有军种作战司令部转

型为完全功能化、具有联合指挥控制能力的司令部。同时将有更多可快速部署的常设联合特遣部队司令部供作战司令部司令官使用。这些联合司令部可对作战、情报等进行实时分析, 提高联合部队的作战适应能力和行动速度。

### 3.2 制定实现联合通信与指控能力的指导方针

#### 3.2.1 强化对“任务能力”的管理

“任务能力”是执行防务作战任务或者类似战区防空或远程精确打击任务的实际能力。这些能力依赖于一系列相关的系统, 如多系统集成之系统。该能力不仅依靠装备系统, 还依赖于有关的条令、机构、训练、装备、领导力和人员。所有这些要素需“共同开发”并综合集成以生成一种实际能力。

为此, 美军制定“任务能力”管理体系结构, 以便在联合任务域内和联合任务域间, 以集成、同步的方法管理上述各要素来提升联合作战和支持能力。

#### 3.2.2 将互操作能力贯穿于开发的各个阶段

互操作能力的开发问题贯穿于从构思一直到螺旋式发展整个过程的任一阶段。只有在各个阶段制定能够提高并保护互操作能力的方法, 才有开发出真正实现互操作的系统, 实现有效的任务能力。为此, 美军采取了一系列具体的指导方针。

### 3.3 制定实现联合指控与通信能力的方案

美军为了实现联合指控与通信能力, 提出了一系列有关装备与技术方面的方案。

- 明确全球信息网格计划, 通过顶层需求文件发布初步方针和政策备忘录, 构建基线体系结构。
- 改进联合需求程序, 将互连互通互操作能力作为关键性能参数。
- 确定联合分发工程设备, 为 C<sup>4</sup>I 体系结构提供试验床。该方法采用的是已投入使用或正在研发的系统复制品。
- 创建单个集成空中图像系统工程, 以协调多系统集成之系统的工程开发, 包括提供联合空中图像的传感器、通信系统及计算机。
- 制定互连互通互操作作战图像系列方案, 通过三个支柱, 即联合数据策略、汇合

（轨迹与传感器）以及多级安全为相关的国防部以及在战术级实现互连互通互操作提供一个方向矢量。

## 4 美军实现联合通信与指挥控制系统能力个案

### 4.1 伊拉克战争检验美军联合通信与指挥控制能力

#### 4.1.1 21 世纪部队旅和旅以下作战指挥系统发挥作用

伊拉克战争中，美陆军第 4 机步师的 3 个旅中有 2 个旅配备了 21 世纪部队旅和旅以下作战指挥系统，每个旅 300 套。其他部队每个师配备 100—200 套，平均每 10 辆车中有 1 辆安装了该系统。海军陆战队配备了 150 套，英军侦察车配备了 50 套，美陆军第 3 机步师后来也配备了此系统。美军之所以部署了数量如此之多的 21 世纪部队旅和旅以下作战指挥系统，是因为该系统在交战中表现出了卓越的性能。首先，21 世纪部队旅和旅以下作战指挥系统为部队提供了高度的态势感知能力。以前军事作战必须依靠指挥官使用无线电台在其指挥位置上反复呼叫来实施，有了 21 世纪部队旅和旅以下作战指挥系统，任何师级指挥人员只需 2 分钟（而不是以前的 15 分钟）就可以通过屏幕知道下级指挥官的位置或者前线部队正在做什么，这大大增加了态势感知和实施联合作战的能力。此外，21 世纪部队旅和旅以下作战指挥系统还使美陆军地面车辆、飞机和指挥中心能够在同一时间近实时地看到同一幅综合战场态势图，并利用无线电和卫星通信，根据单兵输入的信息不断更新战场态势图。其次，21 世纪部队旅和旅以下作战指挥系统还具有可靠的信息传输能力。它可以与陆军的高层战术通信系统相连，允许士兵把收集到的情报向上反馈给通用作战态势图，供驻多哈营地的美军指挥官和五角大楼的陆军参谋长每天查看。第三，21 世纪部队旅和旅以下作战指挥系统还能有效地减少误伤。据统计，误伤率从海湾战争的 24% 降低到伊拉克战争主要作战阶段的 11%，装备了 21 世纪部队旅和旅以下作战指挥系统的部队更是无一误伤。

参考文献（略）

作者联系方式

通信地址：北京丰台大成路 13 号 X01

邮政编码：100039

联系电话：820343

#### 4.1.2 “联合网络传输能力”系统取代“移动用户设备”

伊拉克战争中，美军的通信能力基本满足了伊拉克战争对通信的“爆炸性需求”。但是实战中也暴露出美军战场和战术通信存在很多问题，参战部队认为战略通信保障虽然较好，但是战役级尤其是战术级通信的漏洞很多，如 20 世纪 80 年代投入使用的移动用户设备，覆盖范围和移动通信能力难以满足运动中的联合作战要求；单信道地面与机载无线电系统等战场电台在城市环境中对障碍物的穿越能力、使用距离和抗干扰能力不够；现役的二十多种无线电台采用多种工作频段和工作体制，难以实现互连互通等。为了解决上述问题，美陆军原计划用战术级作战人员信息网取代移动用户设备。战术级作战人员信息网是陆军未来的战术内联网，能提供真正的“动中通”能力、自愈网络和未来作战所需的带宽。但是目前战术级作战人员信息网有些技术还不成熟，其发展有一定的不确定因素，短期内还难以投入实战。于是美军快速采购了联合网络传输能力系统，作为现装备的移动用户设备和未来战术级作战人员信息网之间的桥梁，部署到参加伊战的第 3 机步师。

### 4.2 “联合武士互操作演示”加强美军与盟军互操作能力

为了提高联合指挥控制和通信能力，美军采取了多方合作、协同发展的策略。从上个世纪 80 年代初，美军就建立了陆海空三军联合通信实验中心，从 90 年代中期开始，每年都要举行三军“联合武士互操作演示”，其目的在于促进海陆空三军信息系统的协同发展，加强其互通性和互操作性。

互通试验是在一种综合作战环境下进行的，以便帮助确定提供给作战人员及应急人员的能力的有效性。过去，军方只是从演示中各公司展示的新系统和互操作性解决方案中挑选少数几项技术进行深入研究。从 2002 年联合武士互操作演示开始，演示的宗旨发生变化，更多地以作战为重点，更多地侧重那些能够在演示结束之后快速交付的能力。

# 军用计算机网络发展趋势探讨

张磊 戴浩 马明凯 刘建军

**摘 要:** 分析了军用计算机网络的特点, 重点介绍了与民用计算机网络的不同之处, 在此基础上, 探讨了军用计算机网络的发展趋势, 重点分析了安全性、服务保障等方面的发展趋势, 对军用计算机网络的发展具有一定的参考意义。

**关键词:** 军用计算机网络; 网络安全; 复杂电磁环境; 网络生存性

## 1 引言

现代计算机网络实际上是 20 世纪 60 年代美苏冷战的产物, 是美国为提高电路交换网络的战争生存性而构建的分组交换网络, 最早的分组交换网络是美国的军用计算机网络 ARPANET, 这个网络后来分为目前的因特网的前身和美军的计算机网络<sup>[1]</sup>。近年来, 计算机网络技术的飞速发展, 不仅给民用计算机网络带来了产业繁荣, 也给军用计算机网络的发展提供了很好的借鉴。军用计算机网络用于保障军队作战指挥、作战保障及日常办公、业务、训练、教育等任务, 由于功能需求的不同, 军用计算机网络相比于民用计算机网络有其自身的特点。

在我国, 军用计算机网络和民用计算机网络采取了物理隔离措施, 与民用计算机网络相比, 军用计算机网络加入了一些较为严格的运行管理规定, 有些时候通过行政管理手段加强对网络运行的管理。随着现代战争对军事能力的需求不断提升, 军用计算机网络的基础性作用更加突出, 本文主要研究军用计算机网络的特点, 并分析其发展趋势。

## 2 军用计算机网络特点及分析

自 20 世纪 80 年代以来, 民用计算机网络技术迅猛发展, 计算机网络技术给整个人类文明和社会进步带来了巨大和深刻的影响, 与此同时, 针对计算机网络的研究也蓬勃发展, 军用计算机网络作为军队建设的基础信息设施, 其特点也开始引起军队以及军工企业研究机构的重视。

以美国为首的发达国家, 军队计算机网络比较

先进, 而且远景规划都已经涉及到未来 20 年甚至更长时间的发展。美国国防部建有三个计算机网络, 即保密 IP 路由网、非密 IP 路由网和联合全球情报通信系统 IP 路由网, 它们是国防信息系统网的重要组成部分, 分别支持国防部的秘密、非密但敏感以及机密至绝密级数据业务。

我国的军用计算机网络是根据军事斗争需要建立起来的, 国际上兴起的网络战、网络中心战等一系列军事理论的创新和实践, 引发了中国的新军事革命, 军用计算机网络作为军队信息化的基础设施, 首先引起了大家的重视。针对军用计算机网络出现类似民用计算机网络的问题, 以及一体化联合作战的需要, 我们必须认真考虑军用计算机网络的未来发展, 这需要首先仔细分析军用计算机网络的特点。

与民用计算机网络相比, 军用计算机网络比较突出的特征是“两强”、“两高”, 其中“两强”即强服务、强认知, “两高”即高安全、高机动。“强”、“高”是相比于民用计算机网络而言, 军用计算机网络服务保障能力、认知能力要更高, 安全性、机动能力要更强, 其特点具体分析如下。

(1) 军用计算机网络承载任务意义重大, 要有强服务能力

民用计算机网络, 提供尽力而为型的业务服务质量 (QoS) 保证, 为数据传送类的应用提供无差错的传输及合理的响应时间<sup>[2]</sup>, 没有提供面向多媒体和实时业务所要求的服务质量保证技术, 它虽然也采用综合服务 IntServ、区分服务 DiffServ 等协议保障网络的服务质量 QoS, 但是这些协议所能达到的服务水平不能满足军用计算机网络的需要, 不能适应业务对网络承载多样化的要求, 因为军事情报信息以及与作战相关各种信息对时效性要求很高,

战场态势信息量非常大,包括很多图像和视频信息,网络的服务保障功能要强。强服务能力是对军用计算机网络的总体性能的要求,是面向军事任务的能力要求。宽带高速计算机网络是军用计算机网络的理想传输模型,轻载网络也是一种理想的解决方法,但是,在带宽资源相对紧张的情况下,还应当研究一些适合军用的简单有效的服务质量保障方法。

(2) 军用计算机网络面临复杂的电磁环境,要有强认知能力

民用计算机网络主要采用光纤线路,而军用计算机网络,根据各种需要,组织方式多样,除了固定网络外,还有无线方式组织的各种作战、指挥、训练所用网络,无线设备所处的电磁环境非常复杂。复杂电磁环境主要来源于三个方面,一是“敌扰”,敌方利用电磁干扰技术,在特定时间、特定地域所进行的通信干扰,“敌扰”使得被干扰的无线网络的链路可用性受到破坏。二是“自扰”,作战部队在一定区域所用的无线设备很多,各设备之间所采用的频率由于频谱利用率的关系,经常出现重叠,没有严格高效的频谱管理机制,“自扰”现象也会造成严重的后果。三是“天扰”,就是某些自然现象,如闪电、雷击等对无线通信设备造成的影响,这种干扰时间短,但是强度大,也是复杂电磁环境的一个组成部分。这种复杂的电磁环境给计算机网络设备之间的通信带来了很大影响,信息传输误码率增大,甚至在“敌扰”严重时,有些链路无法完成通信,这与民用计算机网络的电磁环境差异很大。

军用计算机网络要在这样的复杂电磁环境中保障通信任务,除了利用信号处理技术研究各种抗干扰方法,还应当研究在复杂电磁环境下,利用“抗隙通信”等方式实现最低限度通信,使敌干扰达不到阻断通信链路的目的。而认知无线电技术是针对复杂电磁环境提出的一项技术,它以系统工程方法论、信息处理技术与计算机科学中人工智能为基础,旨在解决无线通信网络的环境自适应问题,将成为新一代军用无线通信系统不可或缺的关键技术之一,并在认知无线电技术基础上逐渐发展认知网络,增强军用计算机网络的认知能力。

(3) 军用计算机网络安全威胁特殊,要有高安全性要求

军用的计算机网络和民用计算机网络的组织结

构是相似的,采用的也都是 TCP/IP 协议,只是大多军用计算机网络与民用的计算机网络物理隔离,采用网内独立统一的地址编码。因此,军用计算机网络面临的安全威胁与民用计算机网络有很多相似之处,例如病毒、DDoS 攻击、操作系统漏洞攻击等。但军用计算机网络具有比较严格的运行管理规定,民用计算机网络中的一些安全问题,在军用计算机网络中并不突出,如网络赌博、侵犯知识产权、以盈利为目的的网络攻击、经济犯罪、“僵尸网络”等。军用计算机网络中出现的病毒也大多是通过移动存储设备从民用计算机网络中带来的。这些情况决定了民用计算机网络中的安全防护以及病毒防护方法在军用计算机网络中同样适用。

实际情况表明,来自军用计算机网络内部的安全威胁相比于民用计算机网络要少的多,而更大的安全威胁来自于敌方有组织的网络攻击,这种网络对抗环境下的攻击,往往攻击强度比较大,目标总是针对机密性高的网络节点或链路,造成的网络问题也是比较严重的。对于这种网络攻击的防护要求军用计算机网络具有非常高的安全保障措施,从接入网认证,到防火墙、入侵检测等多种安全措施配合使用。

在军事计算机网络安全防护上,除了借鉴这些民用计算机网络的安全防护手段外,还要针对军用计算机网络自身特点,充分发挥运行管理及行政管理方面的作用,以弥补 IP 网络在安全方面的先天不足。此外,还应当针对军事应用需求,从网络体系结构到网络协议等方面,积极开展新一代军用计算机网络技术研究。

(4) 军用计算机网络机动性高,要有快速组网能力

军队各种武器系统、信息系统和指挥控制系统都需要军用计算机网络实现互联,网络将成为未来信息化战争的中心。平时军用计算机网络以固定网络为主,除了演习或训练所要求的网络外,军用计算机网络拓扑比较固定,这种网络要求具有高顽存性,在部分节点遭受对方硬打击时,其余网络节点和链路能自动重新组网,保证基本通信的可用性。

而在战时,由于野战通信的需要,军用计算机网络对机动组网要求比较高,军用计算机网络面临被敌方破坏的危险,在部分节点或链路遭受硬打击或网络攻击后,快速有效移动节点,及时恢复网络成为军用计算机网络的重要特点。此外,战时搭载

在各种武器装备上的网络设备, 移动性非常高, 因此, 军用计算机网络还必须有强大的无线组网、快速重组等功能, 以适应瞬息万变的战场态势。

除此之外, 与民用计算机网络相比, 军用计算机网络在某些方面具有一定的优势, 首先, 军用计算机网络是有组织、有纪律、有警察的虚拟世界, 它不崇尚无政府主义, 不以保护个人隐私为目的<sup>[3]</sup>, 这就给管理带来很多方便, 安全问题也可以溯源; 其次, 在军用计算机网络上运行的应用具有相对一致性, 主要围绕军队各项任务来开发应用, 运营管理相对简单; 第三, 军用计算机网络是由军队信息化管理部门统一协调设计和建设, 军队组织管理机构的严格管理, 使得网络建设更易协调, 采用步调一致的行动更容易, 有利于军用计算机网络的规划和建设。

对军用计算机网络的特点进行分析, 掌握其现状以及作战、训练对计算机网络的功能需求, 可以为我们研究军用计算机网络的发展趋势提供依据。

### 3 军用计算机网络发展趋势分析

目前, 军用计算机网络正处于变革的时期, 各国军队也都在积极开展研究论证, 确保军用计算机网络成为未来战争的中心, 服务于未来信息化作战。根据上一节对军用计算机网络的特点分析, 我们得出了军用计算机网络发展的几个趋势。

第一, 军用计算机网络应当保留和加强面向连接的通信方式。就目前以及可以预见的今后一段时间里, IP 网络还是军用计算机网络的主要组织形式, 其安全问题还是很难有根本的解决, 固有的尽力而为的服务方式很难保证某些军事应用的需求, 所以, 在军用计算机网络中, 对于时效性、机密性等要求比较高的业务和任务, 应当使用面向连接的通信方式, 这种通信方式的典型例子就是固定电话网络, 其安全性是非常高的。多协议标记交换(MPLS)技术就是应用在 IP 网络上的面向连接的信息传递技术, 它可以大大提高网络的业务服务质量, 但是对于安全性问题, 其作为并不突出, 因此, 适用性强的面向连接的通信技术将是军用计算机网络的一个杀手铜技术, 也是军用计算机网络技术的发展方向之一。

第二, 军用计算机网络的生存能力将大大增强。计算机网络最早就是美国军方为了增强通信系

统的生存性而设计的, 目的是防止由于部分节点的失效而导致整个网络瘫痪。计算机网络的生存性在被人们忽略了多年以后, 面对当今网络出现的一些问题, 网络生存性又引起了人们的重视, 尤其是在军用计算机网络的研究中。网络生存性研究的内容非常广泛, 它集成了可靠性技术、安全性技术、认知网络技术等多方面内容, 目的是构造一个适用于军事应用需求的网络。

第三, 军用计算机网络将向分等级、多样化的方向发展。根据军用计算机网络的功能定位、使用对象等方面的不同, 单一的综合集成的网络形态不能满足军事应用的各种需要, 前文已经介绍过, 美国国防部也建有保密 IP 路由网、非密 IP 路由网和联合全球情报通信系统 IP 路由网三个相互独立的网络。我军的电话网就是按密级分为密话网和公用网, 在军用计算机网络的发展过程中也存在有分等级、多样化的趋势。

除了以上技术层面的发展趋势之外, 在军用计算机网络的发展思路上也应当有所考虑。例如, 军用计算机网络的功能可以在平时演习或网上对抗实战中不断完善, 由于网络对抗的演习费用很低, 不会对硬件造成损伤, 在这样的有利条件下, 可以开展实战状态下的军用计算机网络对抗演习, 减小军队平时和战时的环境差异, 更有利于实战中发挥各种装备的效能, 在演习中发现军用计算机网络存在的问题, 不断改进, 形成良性循环。

此外, 由于民用计算机网络资源丰富, 网络规模巨大, 在必要的时候, 可以作为军用计算机网络的后备资源。在历次现代化高技术战争中, 民用技术应用到军事上的例子屡见不鲜, 这也是军用计算机网络技术发展的广泛资源, 为军用计算机网络的发展提供技术选择的余地。

### 4 结束语

军用计算机网络是根据民用计算机网络建造起来的, 但是它也有自身的特点, 我们应当加强适合军用网络的新技术研究和民用技术的军事应用改造研究, 建设我军强大的军用计算机网络, 为一体化联合作战建造良好的信息基础设施。

虽然军用计算机网络的原理、基础协议和民用计算机网络区别不大, 但是军用计算机网络特殊的用途决定了它与民用计算机网络不同的设计建设方

式，在分析我军计算机网络特点及发展趋势的同时，借鉴外军计算机网络的发展经验教训，对军用计算机网络的合理健康发展具有重要意义。

### 参考文献

- [1] 谢希仁. 计算机网络. 大连: 大连理工大学出版社, 2000.6
- [2] 刘建军. 下一代网络服务质量研究. 北京理工大学博士论文, 2006.5
- [3] 戴浩. 对我军计算机网络发展的几点思考. 中国通信学会国防通信技术委员会第四届年会学术研讨会议论文集, 2007.9

### 作者联系方式

通信地址: 北京市清河小营东路 2 号院处理中心一室

邮政编码: 100085

联系电话: 010-66820383 15910549202

# 信息化条件下我军心理战飞机发展刍议

张燎 王宣刚 程建

**摘 要:** 本文介绍了美军心理战飞机的使用情况,并分析了近几场高技术条件下局部战争中心理战飞机的使用效果,对我军大力发展心理战飞机的可行性进行了论述,并提出了几点思考意见,对我军心理战武器装备的发展及军队信息化建设具有一定指导意义。

**关键词:** 信息化; 心理战; 心理战飞机

## 1 引言

在军事技术逐渐由机械化过渡到信息化高速发展的今天,心理战仍不失其“攻心为上,心战为上”的重要地位,并已逐步发展成为超然于陆、海、空、天、电之上,与国家战略密切相融的新的作战方式。信息化条件下的心理战场,对制信息权的争夺已成白热化态势,并对战争的进程及结果起着举足轻重的作用。在美军参与的近几场高技术条件下的局部战争中,心理战贯穿全局,尤其对心理战飞机的使用更是频繁,对夺取制信息权和赢得信息化战争的胜利意义非浅。他山之石,可以攻玉。我军也应积极借鉴外军的成功经验,结合自身特色,努力发展自己的心理战飞机,为扎实做好各项军事斗争准备奠定物质基础。

## 2 美军心理战飞机发展现状

### 2.1 美军心理战飞机基本情况

美军发展心理战飞机已有三四十年的历史,并在近几场高技术条件下的局部战争中多次使用心理战飞机,已形成战斗力。据《美国空军杂志》之“2004 年空军装备年鉴”报道,美军现在拥有 7 架心理战飞机,其中 2 架是 EC-130E,代号为“Commando Solo II”(突击队独奏 II); 5 架为 EC-130J,代号为“Commando Solo III”(突击队独奏 III)。因此,美军心理战飞机的发展现状及趋势,一是美军的心理战飞机正在由 EC-130E 向 EC-130J 过渡。EC-130E 与 EC-130J 的最大不同在于载机不一样。EC-130E 以 C-130E 为载机;而 EC-130J 则以 C-130J 为载机。C-130J 比 C-130E 更

大,载油量更多,续航时间也更长。与早期的 C-130E 相比,C-130J 的速度提高了 21%,巡航高度增长了 40%,航程增长了 40%。C-130J 的先进性还体现在发动机、数字化航空电子设备、任务计算机系统等方面的改进。此外,C-130J 的可靠性和维护性也有所提高。二是在散发传单和小批量物品投放方面,美军计划采用无人机。美国特种作战司令部对发展心理战无人机感兴趣,拟大批采购“雪雁”无人机。因为无人机能够扩大心理战的作用范围,向敌纵深发展时能够避免人员伤亡。另外,无人机价格低廉,可重复使用,且操作简单,机动灵活,部署快。

### 2.2 美军心理战飞机已知的任务系统

美军的 EC-130E/J 心理战飞机主要是在载机机舱内加装任务设备,即各种广播设备而成。EC-130E 任务设备的总重量为 13608 千克,其中包括 60/90 千伏安发电机组;设在舱内两侧的操作员控制台,控制台装有 3/4 英寸多制式视频磁带机和 NTSC 视频磁带机、1/2 英寸多制式视频磁带机、光盘播放机、电视制式转换设备、视频分析仪、矢量显示器和彩色电视监视器等设备;多制式电视激励器和接收机、字符产生器、上变频器、发射机遥控装置等设备;以及 AM 广播分系统、FM 广播分系统、TV 广播分系统、接收/分析分系统、自卫辅助分系统和发射/接收天线阵。天线阵由水平拖曳天线、垂直拖曳天线、4 个 VHF“低端”天线(TV 2~6 频道,安装在垂直尾翼上)和 2 个 VHF(TV 7~13 频道)/UHF(TV 14~78 频道)以及天线吊舱(安装在机翼下)组成。



### 3 信息化条件下大力发展我军心理战飞机势在必行

#### 3.1 从近几场信息化局部战争看，运用心理战飞机效果明显

在海湾战争中，美军有三架 EC-130E 一直承担着向伊军和居民进行宣传，促使伊军放下武器的任务。为了配合此次宣传，战前，美军就把数千台小收音机偷运进伊拉克，无偿赠送给伊拉克人，使他们能够收听到美军的心理战广播。据统计，在“沙漠盾牌”行动中，美军使用 EC-130E 心理战飞机连续工作 60 天，每天广播长达 14 个小时，对瓦解敌军官兵心理防线起到了十分重要的作用。在科索沃战争中，美军采用 EC-130E 心理战飞机在 70 多天里，飞行约 80 个架次进行心理战活动。在海湾战争之后，一位伊拉克军队的师长说，心理战对伊军部队的士气是一极大威胁，其威力仅次于联军的轰炸。在伊拉克战争中，美军通过心理战飞机，专设广播电台，每天以 5 种不同频率，使当地军民能在每天 18 点至 23 点，在 5 种波段收听到美军的心理战宣传。其宣传内容抓住伊军和民众的心理弱点，进行有针对性的说服诱导，对于削弱伊拉克军民的抵抗意志起到了积极的促进作用。由此可见，心理战飞机的运用效果明显，我军心理战专业力量建设的现阶段紧迫任务就是研制符合我军特色和未来实战需要的心理战飞机，做到上级统揽，各部门积极配合，并制定出心理战飞机研制和装备部队的时间表。

#### 3.2 以新军事变革为大背景，加快心理战飞机发展切实可行

一是新军事变革浪潮的推动。当前，各国军队都在积极推进军队信息化建设。外国军队，尤其是发达国家的军队，在武器装备建设过程中，坚持“硬、软”杀伤性武器一起抓，对心理战装备建设的认识也在不断增强，为指导心理战装备的建设许多国家都设有专门机构，集中领导，统一协调。据有关资料报道，目前，美国、英国、法国、德国、以色列、叙利亚等国都设有心理战专职机构，指导心理战力量的建设。台湾当局也建立了专门的心理战机构，并从美国引进相关技术与装备组装心理战飞机。

二是我军历来具有实施心理战传统和经验。除了国际大环境促使我军增强心理战能力外，我军在运用心理战分化瓦解敌人方面，历来具有政治工作的强大优势和光荣传统，并积累了相当的经验。面对未来战争需求，我军应当紧跟时代步伐，充分利用先进技术，积极开发新的心理战手段，使我军政治工作的传统发扬光大。

三是我军具备研发心理战飞机的物质基础。我军现有众多的各类飞机，他们为选择心理战载机提供了可能。在技术方面，我国有关心理战飞机所要采用的技术和设备已经比较成熟，如广播设备、遥控遥测设备等，国内许多厂家已有货架产品可供技术改造和支持；天线和设备小型化等技术难点也可通过联合攻关得到解决。所有这些，都为我军发展心理战飞机提供了良好的条件。

### 4 信息化条件下大力发展我军心理战飞机的几点思考

我军心理战的专业研究起步较晚，主要停留在定性的理论和传统的心理战作战手段的研究。虽然近几年在一些领域有所突破，但与西方发达国家相比还存在以下不足：第一，手段与应用的研究少，高水平的仿真模拟、应用研究更少。第二，现行的有关心理战的研究力量分散，理论不系统。第三，组织指挥体系和训练机构还不完善。第四，我军心理战力量一直走以政治机关和政工干部为主体，发挥全军指战员参战的非专业化道路。但是，要想把心理战的专业力量形成战斗力，具备心理战专业武器装备不可或缺。我军心理战飞机的研制工作刚刚起步，当今心理战的高技术化、专业化趋势越来越明显，如不能尽早研制出我军自己的心理战飞机，尽快形成有效战斗力，则必将影响和制约心理战的运用和效果，在未来信息化战争中处于被动局面。也只有在现阶段加大、加快心理战飞机的研究力度，才能对未来实战中的心理战战法和理论研究提供物质基础和实质参照。

#### 4.1 确立正确原则，指导心理战武器装备发展

我军发展心理战飞机应当确立正确原则，整体规划论证，分阶段稳步实施，力争尽快填补我军心理战飞机空白。一是通过模仿求先行。从军事装备

的科研规律来看,70%的活动用在研究、论证、设计方面,30%的活动用在生产实验方面,采取模仿的手段就可以节省70%的时间、精力和资金的投入。我军可以模仿外军的先进心理战飞机,加上自己的技术支持,大大缩短研制周期,立足我军现有装备资源,研制能够实现心理战效果最大化的心理战飞机;二是通过选择求实际。在统筹规划发展心理战飞机的前提下,根据我军现有条件,分清主次,重点选择好能够保证我军实施心理战需要的载机,研发心理战飞机;三是通过兼容求效能。心理战飞机的研制要军民结合、军地兼容,发挥各自优势,充分利用地方科研力量的技术和人才优势,对心理战飞机信号覆盖范围,信号的连续性、完整性、抗干扰能力等方面共同攻关,使心理战飞机机载设备力求做到功能合理,系统配套,使用灵活,维修方便。

## 4.2 建立心理战部队,培养专业心理战人才

美军之所以取得心理战行动的成功,除了有功能齐全的心理战装备外,还有专业化的心理战部队作支撑。我军也应尽快建立具有自己特色的高质量心理战专业部队,适应国际斗争和信息化战争要求,走“集中建设,区域化使用”的道路。尤其对于心理战飞机的使用,可在空军设立特种飞机作战大队,通过训练、演习,摸索出适合我军作战的心理战飞机空中战法和最大效能的提高心理战飞机的优势。另外,我军还应当加强专业心理战人才的培养工作,使我军心理战人才逐步走上高起点的开发之路。通过直接引进、定向培训、军地共育等渠道培养我军心理战建设的骨干力量,为更好的使用心理战武器装备提供可靠保障。

## 4.3 有系统性的实施心理战一体化训练

在今年的全军军事训练会议上,胡锦涛主席发表了题为《推进军事训练向信息化转变》的讲话,

参考文献(略)

作者联系方式

通信地址:陕西西安洋镐东路1号176分号空军工程大学电讯工程学院信息战教研室

邮政编码:710077

联系电话:13891855240

并着重指出:信息化条件下局部战争是体系与体系的对抗,基本作战形式是一体化联合作战。联战必须联训。要着眼提高诸军兵种一体化联合作战能力,大力加强联合训练。因此,我军在改善心理战训练方式上应有系统地抓好一体化训练工作,抓好战略战役战术各个层次的联合训练,并积极探索军政军民联合训练的有效机制和方法,为未来心理战飞机的使用形成合力。在指挥体制上,应把军队心理战列入联合作战指挥序列,以便让指挥员了解军事作战意图、战争进程、作战目的、兵力部署和敌我态势;在战法运用上,要把心理战作为一种创新和重要的战法进行研究和运用,充分发挥心理战在信息化战争中的作用,使之能够影响战争的进程和结局。要制定切实可行的心理战联合作战行动预案,明确心理战飞机支援的时机、手段、要点、切入点和联合作战的任务、保障、组织协同规定等,并自觉将其纳入战役战斗演习的全过程,提高我军心理战联合作战一体化的能力,演练信息化条件下军队心理战的高科技战法,充分发挥未来信息化战场心理战飞机使用的最大效能。

## 5 结论

心理战将成为信息化战争中相对独立的一种作战样式。随着信息技术的快速发展,心理战的作战手段及武器装备都区别于传统心理战的战场喊话和传单投送,越来越体现信息化战场的特点。将大功率的广播、电视设备装在飞机上,便形成了心理战飞机,同时利用飞机良好的机动性,使军队能够可按其作战意图随意部署,让敌方不得不听到、看到己方的心理宣传,实现了心理攻击效果的最优化。积极发展我军心理战飞机研究,加速进行心理战飞机的研制工作,对我军在未来信息化战场赢得制信息权及做好各项军事斗争准备有着重大意义。

# 信息资源开发利用是军队信息化的核心任务

张新强 任刚

**摘 要:** 本文分析了信息资源开发利用的内涵,探讨了信息资源开发利用的重要性,提出以信息资源开发利用为核心发展军队信息化的观点,并就信息资源开发利用思路作了若干建议。

**关键词:** 信息资源; 开发利用; 信息化

## 1 引言

在工业时代,机械化军队的核心战斗力是火力和机动力,辅助战斗力是信息力;在信息时代,信息化军队的核心战斗力是信息力,辅助战斗力是火力和机动力。因此,信息化建设是中国特色新军事变革的重要内容,而军队信息化的核心是信息资源的开发利用,目的是使“信息力”成为军队战斗力的主导性构成要素。

“信息力”是信息资源可利用性的表征。信息资源开发的最终目的是形成信息产品。信息产品有多种类型,可分为简单的原始型信息产品、复杂的知识型信息产品和实用的专业化信息产品。信息资源的利用,即指通过信息系统等手段,实现信息产品的共享,达到作战单元对作战意图、战场态势等共同感知,从而实现精确指挥、精确打击。基本上可以这样说,军队信息化建设的过程就是广义上信息资源开发利用的过程。哪个国家的军队能有效地开发利用信息资源,它就能高效率地推进军队信息化建设。

## 2 军队信息资源开发利用的内涵

军队信息化,是指在国家和军队的统一规划和组织下,以信息化战争的军事需求为牵引,在国家军事的各个领域广泛应用信息技术,有效开发和利用相关的信息资源,使信息技术在军队建设中占据核心和支配地位,在数量和质量上达到军队信息化建设标准的过程。其宗旨就是以数字化、网络化推进信息技术和信息资源的开发利用,大幅度地提高战斗力,改进作战方式和质量。数字化和网络化就是把各类海量信息有组织地“装”在联网的计算机中,是信息化必要的技术基础。信息化是人类历史上的新生事物,没有现成的理论,也没有可以借鉴的成熟经验。信息化建设的开拓者—陆军参谋长沙利文上将指出:“必须改变工业时代围绕火力和机动力筹划军队建设的旧观念,确立以信息为基础建设军队的新思想,让信息主导军队建设”。

所谓军队信息资源是指,可供各作战领域(包括指控、情报、通信、政工、后勤和装备等)直接或间接开发利用的各种数据、信息。信息资源分为两种,一种是未经加工的原始性信息资源,另一种是经过主体感知和加工的信息资源。“开发与组

## 3 军队信息资源开发利用的重要性

### 3.1 信息资源开发利用是衡量军队信息化水平的重要标志

信息资源开发利用是一个整体性的任务,其实现手段上涉及各个领域、学科的知识和技术,是各种知识和技术的综合运用与集成,需要打破军队各部门的界限,统一标准,相互协调,联合行动,任何一个部门、任何一个单位都很难包揽信息资源的开发利用。各类信息资源(包括作战基础数据、情报、通信、后勤、装备等数据和信息)有效开发利用对提升战斗力水平起到了主导性作用,成为衡量军队信息化水平的重要标志。可以从三个方面来衡量军队信息资源开发利用的程度:一是基础数据的统一性,主要是指人员、装备、物资、弹药的数据结构及其内码保持一致,为信息资源开发利用奠定基础,属于信息资源开发利用的基础级;二是战场信息的共享性,主要是指以指挥信息为主体,包括情报等各种保障信息的实时共享能力,是信息资源开发利用的中间级;三是作战人员认知的一致性,主要是指作战人员利用共享的信息产品,达到认识

上的一致,从而实现精确指挥、精确保障、自主协同。目前,美军正在积极开展的网络中心战概念及其支撑系统(GIG)研究,就是以实现信息资源开发利用的最高级为最终目的。

### 3.2 信息资源开发利用是军队信息化建设取得实效的关键

我军自上世纪九十年代推进军队信息化以来,取得了明显的成绩,但是信息资源开发利用一直是我军信息化的薄弱环节,成为军队信息化建设的瓶颈。究其原因,主要有三点:一是观念没有更新,普遍存在“重硬轻软”和“重网络轻信息”现象,特别是后者表现更为严重,很多单位只是用计算机系统简单替代传统的手工作业处理,而忽略后台数据库完善和资料数字化工作;二是信息“私有化”现象严重,一些单位、部门和个人把掌握的数据、资料信息当作一种权利,不愿提供出来共享;三是各部门的信息化建设缺乏统一的规划和标准,各自为政,在“封闭”状态下按照自定的一套规则开发,基础数据结构不一致,导致系统间数据无法交换,最终成为一个个“信息孤岛”。如何打破这一瓶颈?是将一切推倒重来,还是维持现状?显然采取废旧系统,上新系统的方法是不现实的。正确的方法是以信息资源开发利用为核心,强调信息资源的统一规划和管理,对与标准不符的数据格式尽可能转换为标准格式,这样才能突破信息资源开发利用这一遏制我军信息化建设的瓶颈,取得实效。

### 3.3 信息资源开发利用是当代各国军队信息化建设的经验总结

在信息与网络时代,时间“缩短”、空间“变小”,这客观上要求作战行动和指挥向更快、更准、更高的方向变化。传统机械化指挥方式存在的决策层次多、决策权高度集中等弊端导致其无法适应现代战争的要求。从上述对比可以看出,传统机械化指挥方式和信息化指挥方式的区别在于信息收集、存贮、加工、传输方式发生了巨大变化,亦即信息资源开发利用的手段发生了变化。在信息化中由于融入计算机、网络通讯等高新技术使得信息资源开发利用变得意义重大。各国军队在信息化实施过程中,都要紧紧抓住信息资源开发利用这条主线,建立信息资源开发利用的有效机制,加大对信息资源开发利用的投入,着力培养作战人员的信息

素质,以提升军队的核心战斗力——信息力。美军为了获得和保持信息优势,开发和建设了联合公共数据库(JCDB),实现了陆、海、空指挥控制系统及各业务系统数据库的集成,极大地提高了美军各个系统间的数据共享能力,为各国军队信息资源开发利用提供了典范。

## 4 军队信息资源开发利用的思路

### 4.1 建立军队信息资源开发利用机制

大力推动军队信息资源开发利用,要以需求牵引,与应用相结合,特别要注重开发利用的机制建设。一是颁布军队信息资源开发利用相关的条令条例法规,从机制上解决信息资源的管理、开发、使用问题,规范信息资源开发利用行为;二是建立军队信息资源开发利用的专门机构,积极开展数据中心试点示范工作,加大战场信息资源的开发力度,建设若干个总部、军区级数据交换中心和一批重点大型数据库,形成支撑作战指挥决策和作战精确保障的基础信息资源。三是制定信息资源开发利用的标准规范,统一基础数据标准,提供统一的信息交换接口,促进信息资源交换与共享。

### 4.2 构建信息资源开发利用统一平台

在信息技术与信息系统发展迅速的今天,构建信息资源开发利用平台是有效进行信息资源开发利用的重要手段。一是构建以数据库为核心的基础数据体系,统筹考虑,严格标准,建成以作战指挥为主,兼顾训练、管理、动员、保障,多军种、多部门共享,各级别、各系统共用的分布式数据基础平台;二是构建以信息服务为主体的服务构件体系,借鉴地方电子政务、商务系统建设和应用的经验,采用面向服务的技术,提供服务构件,按照横向互联、纵向贯通、相互操作的要求,搭建连通司、政、联、装四大机关和军区、集团军、作战师旅三个层次的信息服务平台;三是构建基于知识的应用体系,按照信息资源开发利用的要求,在信息系统中加大对军事知识规则的应用开发,对统建的系统进行功能扩充和完善,对分建的系统进行融合,对自建的系统进行标准化改造,以此来牵动军队信息资源的整合开发,构建符合军事运用逻辑、富含军事知识的高效应用平台。

### 4.3 加强军队信息资源开发利用人才培养

军队信息资源开发利用需要掌握多学科知识、有综合协调指挥能力的专业技术人才，这就要求我们在实际工作中着重培养既掌握军事专业知识又掌握信息技术的复合型人才。在人才培养方式上，一是要依托军事院校或科研机构开设专业的学习课程，提高军事人员的信息素质和技术人员的军事素质；二是发挥各级数据中心的作用，走成体系培养人才的路子；三是广泛采用模拟训练技术，注重在各种演练实践中培养人才。在人才培养内容上，一是，要充分了解目前我军信息资源开发利用的现状，提高对信息资源开发利用的重要性的认识；二是加大对技术保障人员的信息资源开发利用的技术和知识培训，为提供高质量的信息产品打下坚实的技术基础；三是加强对作战人员作战思维和认知培训，实现由信息共享到共同感知的转变，最终形成信息优势。在人才培养机制上，一是建立人才激励机制，激发优秀人才参与信息资源开发利用的积极性和自觉性；二是优化人才成长机制，创造有利用

于高素质人才成长发展的环境条件；三是严格人才管理机制，注重建章立制管理人才，实现信息资源开发利用人才的合理配置和高效利用。

## 5 结束语

信息技术的发展日新月异，为军队信息化建设提供了前所未有的机遇和挑战。我们要清醒地认识到无论从我军信息化发展对信息资源需求来看，还是从目前信息化发展的现状来看，信息资源开发利用仍是一个最薄弱的环节，是信息化发展的瓶颈。我们要高度认识信息资源开发利用在军队信息化中的核心地位，树立信息资源需要开发、信息资源开发需要投入的观念，处理好信息资源共享与安全保密的关系，努力开发，充分利用，全面推进我军信息化建设。

### 参考文献

- [1] 王保存，《世界主要国家信息资源开发利用的启示》，《军事科学研究》2006年第6期
- [2] 李振富等，《信息资源规划问题研究》，军事通信学术委员会，2007年7月

### 作者联系方式

通信地址：北京丰台区大成路13号Z00

邮政编码：100039

联系电话：010-66820125

# 一体化联合作战概念牵引美军向信息化军队转型

张永红 陈宇杰 左琳琳

**摘要:**在向信息时代军队的转型过程中,美军重视开发联合作战概念,将其作为影响转型成功的关键要素。自2003年以来,美军已先后制定了一系列相互衔接、相互补充的联合作战概念文件,勾画出未来的联合部队能力,指导着美军的武器装备建设。本文介绍了美军联合作战概念的组成、作用及相互关系,及其对军事转型的指导作用,总结分析了美军联合作战概念确定的军队建设能力要求,通过联合能力集成与开发系统将联合作战概念转化为装备能力需求的主要方法。

**关键词:**联合作战概念;转型;信息化建设

美军一直十分重视作战理论对军队信息化建设的牵引作用。美军认为,“概念是一种思想的表达,表达如何来完成某项事情。联合作战概念是未来作战的可视化表达。”在向信息时代军队的转型过程中,美军更加重视开发联合作战概念,将其作为影响转型成功的关键要素。“通过开发联合作战概念,一体化联合作战思想得到详细说明,然后通过联合试验和其他评估手段对联合作战概念进行进一步的探索”。因此,美军不断创新联合作战概念,自2003年以来,已先后制定了一系列相互衔接、相互补充的联合作战概念文件,勾画出未来的联合部队能力,指导着美军的武器装备建设。

## 1 一体化作战已成为信息时代美军联合作战的本质特征

1982年,美陆军的“空地一体战”理论标志着美军现代联合作战思想的萌芽,之后,美军不断完善作战理论的管理机制,大力推动联合作战理论的发展。1986年,美国会通过《戈德华特-尼科尔斯国防改组法》,强化了参联会主席和联合司令部司令的权力,明确要求参联会主席负责联合作战理论的研究和制定工作。1991年后,美军开展了以反思海湾战争经验教训为主题的理论创新,参联会先后组织出版的情报、作战、后勤、C4系统等7个系列的联合出版物,成为美军计划、组织和实施联合战役的重要理论依据。1996年和2000年,美参联会相继颁发了《2010年联合设想》和《2020年联合设想》,提出了主宰机动、精确打击、全维防护和聚焦后勤等四大联合作战概念,作为指导美

军联合作战和装备发展的顶层概念。1999年10月,美军将大西洋司令部改为联合部队司令部,负责全军联合作战理论的研究、发展与验证,完善了联合作战理论的开发体制。

近年来,美军在基于能力的军队建设思路指导下,将联合作战概念的开发放在十分重要的战略地位。在2001年《四年一度防务评审》中,将加强联合作战概念的开发与验证作为转型的四大支柱之一。在2003年《转型规划指南》中,进一步强调了联合作战概念开发与验证的重要性。2003年以来,美参联会先后制定并颁布了《联合顶层作战概念》(CCJO)(美军原称为《联合作战概念》)、《联合行动概念》(JOC)、《联合功能概念》(JFC)和《联合集成概念》(JIC)(美军原称为《联合赋能概念》)系列文件。2004年,美参联会在《联合转型路线图》中指出,“开发和继续完善一系列新的联合概念,正在成为创造和保持美国武装部队未来军事能力的奠基石”。2006年,美军在《四年一度防务评审》指出,未来联合部队将“从需要互相协同减少摩擦的联合作战向一体化作战甚至是相互依赖的作战转变”。一体化作战正在成为美军在信息时代联合作战的主要特征。

“一体化作战”一词首先由美原参联会主席理查德·迈尔斯将军在2005年4月的《联合部队季刊》提出,他认为美军“需要将军事竞争力从联合作战向一体化战转变”。据美国防部《军事与相关术语词典》,联合作战是指由联合部队或各军种部队共同实施的军事行动,也就是说联合作战强调的是由军队共同实施的军事行动。根据《联合部队季刊》第5期美国半球国防研究中心主任的文章,一



体化作战更强调参与军事行动单元的多样化。随着美国所面临威胁的多样化,美国军队必须与本国非军事政府机构、非政府组织、企业以及其他国家的军队、政府机构、非政府机构组织联合在一起,在各种军事行动中取得全面优势,包括维和行动、战争和保持长期和平稳定等各种行动。

一体化作战正在成为美军当前联合作战理论探讨的重点,一体化作战的内涵和特点将随着美军研究的不断深入而得到系统全面的阐述。就目前研究结果分析,一体化作战是联合作战的高级发展阶段,是美军为了迎接新的安全环境挑战对联合作战概念和理论的进一步深化。一体化作战的人员构成更加复杂多样,要求将各种要素有机地联系在一起。一体化联合作战与联合作战最大的区别在于,一体化联合作战把各种能力融为一体,联合的内部是顺畅的、协调的;而联合作战只强调各种力量的联合,内部存在需要化解的矛盾。正如迈尔斯将军特别强调的,一体化作战更加强调战场空间管理能力,也就是 C4ISR 系统的一体化能力。一体化作战要求组成战场空间管理系统的所有要素都要协调配合,实现信息的实时收集、融合和共享,以实现更快、更好的战略和战术决策。一体化作战对联合部队提出了更高的要求,要求联合部队向知识化、网络化、可互操作、远征能力强、灵活可裁减、精确、快速与持久作战和能实施致命性打击等方向发展。

## 2 新的联合作战概念提出了未来联合作战的能力要求

目前,美军已制定了由《联合作战顶层概念》为指导,《联合行动概念》、《联合功能概念》和《联合集成概念》相互支撑、相互衔接的系列联合作战概念文件,它们以 2012—2025 年为时间参照点,分别从顶层、作战、功能等角度描述了未来一体化作战的环境、原则和能力等。它们的相互关系如图 1 所示。

《联合作战顶层概念》主要描绘美军在 2012—2025 年之间可能面临的安全环境和军事问题,确定了未来联合部队应具备的特征,明确了未来联合部队应如何作战。《联合作战顶层概念》为开发从属的《联合行动概念》、《联合功能概念》和《联合集成概念》提供了框架,以指导未来联合部队能力的开发。

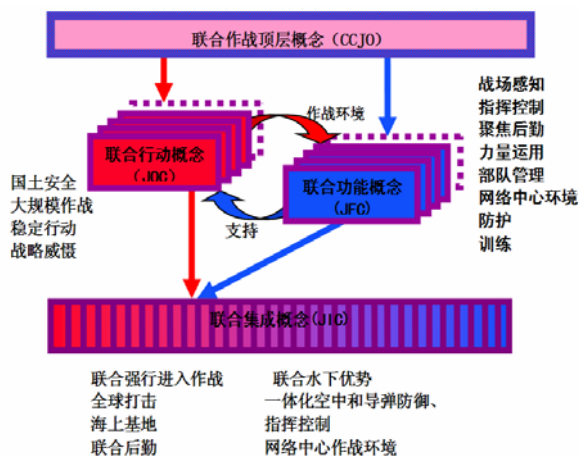


图1 美军系列联合作战概念关系图

《联合行动概念》重点描述特定军事行动中,联合部队指挥官如何规划、准备、部署、运用和保障联合部队,以战胜任何潜在的对手和威胁。美军将联合行动概念称为“转型的发动机”,它进一步描绘了美军在特定的军事行动中,所面临的挑战、解决挑战的方法、要实现的作战目标及所需的能力,以指导《联合功能概念》、《联合集成概念》和各军种作战概念的开发和集成,并为联合试验提供基础。当前,美军已确定了国土安全、大规模作战、稳定行动和战略威慑四个联合行动概念。

《联合功能概念》描述未来联合部队如何完成特定的军事功能,确定实现联合行动概念及支持未来联合部队作战所必需的功能能力和特征,并为开发《联合集成概念》提供框架。目前,美军已颁布了战场感知、指挥控制、聚焦后勤、力量运用、部队管理、网络中心环境、防护和训练 8 个联合功能概念文件。

《联合集成概念》是《联合行动概念》和《联合功能概念》的“子集”,针对的是更低层级的联合能力域,集中解决联合行动概念或联合功能概念中某个行动或功能中的问题,进一步细化了未来联合部队所需的能力。当前,美军已制定了 8 个联合集成概念文件:联合强行进入作战、联合水下优势、全球打击、一体化空中和导弹防御、海上基地、指挥控制、联合后勤和网络中心作战环境。

除了《顶层联合作战概念》,每个联合作战概念文件,都从不同侧面、不同角度、不同层次提出了相关作战概念的能力要求。这些能力有的是针对部队编制的要求,有的是对装备的能力要求,能力之间相互交叉,互为补充和支撑。每个联合功能概念和联合集成概念又对某一特定能力进行了更为详

细的描述。联合功能概念是完成四种联合行动所需的所有功能，不同功能能力进行组合，就可以支持所有的作战行动。如大规模作战联合行动概念中，提出了指挥控制、战场感知、兵力运用、聚焦后勤等 5 项能力，就对应着五个功能概念。联合集成概念则进一步细化了某一具体行动或功能的能力。美军制订未来装备发展计划时，都要以系列联合作战概念中的能力要求为指导。

3 新的联合作战概念成为美军向信息化转型的重要牵引力

美军的联合作战概念以美国的高层军事和安全

战略为指导，以《国家安全战略》、《国家军事战略》、《国防计划指南》、《转型计划指南》、《四年一度防务评审》和《2020 年联合设想》等为依据进行开发。通过不同层次的联合作战概念文件，综合、全面描述了美国部队未来达成各种政治和军事目的所需的能力和 方法。为了保证军队建设的正确方向，美军还将随时吸纳新思想和新需求，并通过作战实验和评估，动态修订。如《顶层联合作战概念》已于 2003 年、2005 年发布了两版。《联合行动概念》约 2 年更新一次。表 1 为联合作战概念文件的更新情况。

表 1 联合作战概念文件更新情况

文件名称		文件状态	文件制定单位
联合作战顶层概念		2005 年 8 月通过第 2 版	联合试验、转型和概念部
联合行动概念	国土安全	2004 年 2 月 CJCS 批准第一版	北方司令部
	大规模作战	2004 年 9 月 CJCS 批准第一版	联合部队司令部
	稳定行动	2004 年 9 月 CJCS 批准第一版	联合部队司令部
	战略威慑	2004 年 2 月 CJCS 批准第一版	战略司令部
联合功能概念	战场感知	2003 年 10 月 JROC 批准第 2.1 版	联合参谋部情报局
	指挥控制	2004 年 2 月 JROC 批准第 1.0 版	联合参谋部 C4 系统局（J6）
	聚焦后勤	2003 年 12 月 JROC 批准第 1.0 版	陆军和联合参谋部后勤局（J4）
	力量运用	2003 年 12 月 JROC 批准第 1.0 版	联合参谋部部队结构与资源评估局（J8）
	部队管理	正在等待 JROC 批准	联合参谋部部队结构与资源评估局（J8）
	网络中心环境	2005 年 4 月 JROC 批准第 1.0 版	联合参谋部 C4 系统局（J6）
	防护	2004 年 1 月 JROC 批准第 1.0 版	联合参谋部部队结构与资源评估局（J8）
	训练	2005 年 7 月形成第一份草案	联合训练功能能力委员会
联合集成概念	联合强行进入作战		联合部队司令部联合试验局（J9）
	联合水下优势	正在进行功能方案分析	-----
	一体化空中和导弹防御	2005 年 1 月 JCS 批准第 1 版	空军
	全球打击	目前 JCS 已批准第 1 版	空军
	海上基地	2005 年 8 月批准第 1 版	海军
	指挥控制	2005 年 1 月批准第 1 版	联合部队司令部联合试验局（J9）
	联合后勤	2006 年 2 月发布第 1 版	陆军和运输司令部
	网络中心作战环境	2005 年 10 月批准第 1 版	-----

联合概念作为“转型的驱动力”，用于明确转型的范围、目标、能力要求和发展方向，明确未来联合部队需要的能力、组织形式、运用方式和部署态势等，是美军制定转型决策的重要依据。美军将根据联合作战概念系列文件开发联合和各军种转型路线图，制定投资决策，联合作战概念指导美军未来联合部队发展和武器装备的建设。如图 2 所示。

2003 年，美国防部制定并颁发参联会主席指

令 3170.01 系列文件，提出以国防部为主导的、“自上而下”的联合能力集成与开发系统（JCIDS），取代过去以军种为主导的“自下而上”的需求生成系统，如图 3 所示。2005 年，美国防部又更新了上述部分文件，进一步完善了联合能力集成与开发系统，更加突出强调了对联合能力需求的管理。联合能力集成与开发系统强调以美国国家安全战略、军事战略、《联合顶层作战概念》、《联合



行动概念》、《联合功能概念》和《联合集成概念》等系列文件为顶层指导，以一体化体系结构为手段，通过国防部主导的清晰、严谨的需求生成流程，以及《初始能力文件》（ICD）、《能力发展文件》（CDD）和《能力生产文件》（CPD）三个需求

文件的制定和审批，强化国防部在需求生成中的主导地位，保证联合作战概念对装备建设的牵引和指导作用，实现基于能力的军队建设方针。

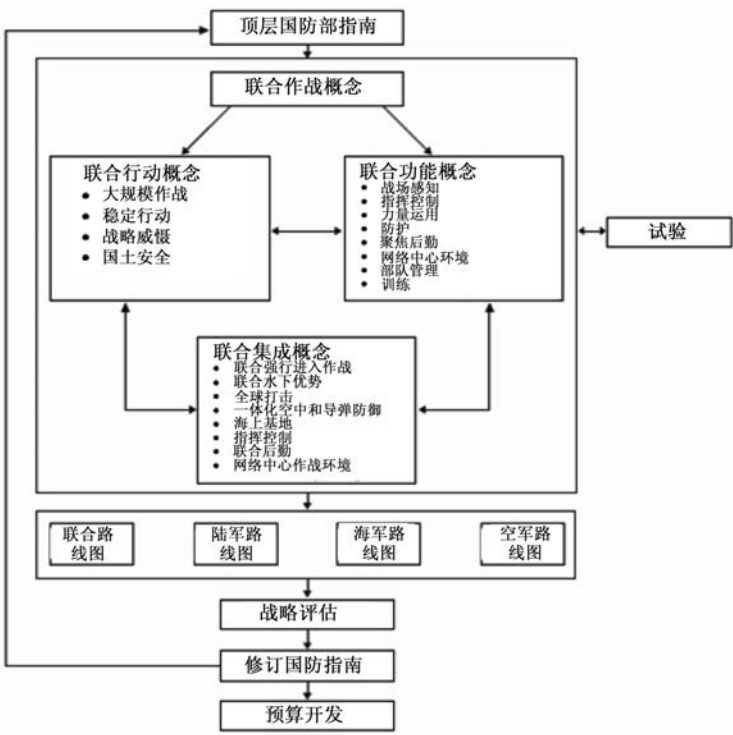


图2 联合作战概念对美军军事转型的指导

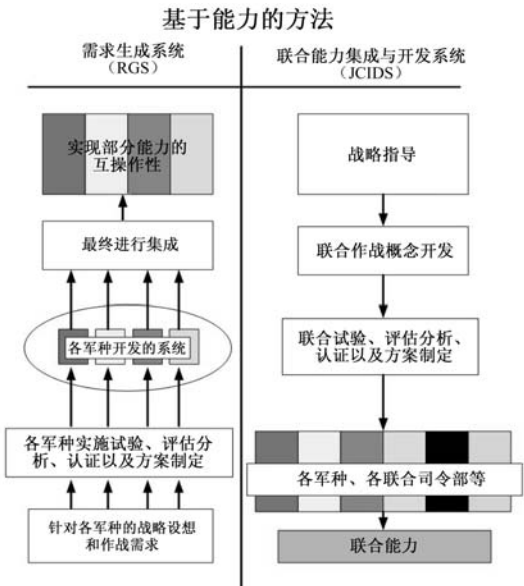


图3 美军两种需求生成机制对比

参考文献（略）

作者联系方式

通信地址：中国国防科技信息中心

邮政编码：100036

联系电话：010-66357093

# 推动网络中心战，美国国防信息系统局扮演重要角色

赵静 孙启辉

**摘要：**美军为了保持在全球的信息优势，一直致力于发展网络中心战。在此过程中，美国国防信息系统局作为国防部一个特殊业务部门，通过致力于实现一系列网络中心目标来推动网络中心战的发展。本文主要介绍国防信息系统局的组织机构、核心任务及其为发展网络中心目标而采取的策略。

**关键词：**国防信息系统局；网络中心战

美国国防信息系统局（DISA）是美国国防部（DoD）一个特殊的业务部门，受主管网络与信息集成（ASD（NII））的助理国防部长直接领导，肩负着为美军信息技术作战提供支持的使命。该局目前共有 6500 人，可调拨资金 60 亿美元。主要负责计划、开发服务于国家指挥当局（NCA）的 C4I 业务。具体工作涉及制订计划、管理工程、操控国防信息系统网（DISN）、采购、部署并支持全球以网络为中心的解决方案，以满足总统、副总统、国防部长、参谋长联席会议、作战指挥官以及国防部其他部门平时与战时的需求，其中全球信息网络（GIG）的运行与防护工作就是由国防信息系统局负责的。该局多年来在组织、管理美军信息化项目实施，推动美军网络中心战能力，保持本国军事领先地位，增强国防实力方面一直发挥着至关重要的作用。

## 1 国防信息系统局的发展和组织机构

国防信息系统局原名国防通信局（DCA），1960 年 5 月 12 日在华盛顿特区成立，当时职员 450 人。其职责是管理国防通信系统（DCS），将陆军、海军和空军的独立远程通信功能予以合并。1991 年更名为国防信息系统局。

国防信息系统局总部位于华盛顿。设有局长、副局长、局长助理以及下列机构：

- 直接报告部门：首席技术官、部门采购执行官、网络企业服务计划办公室和高级顾问；
- 特别顾问：国会事务办公室主任、国防频谱办公室主任、联合互操作能力测试部

（JITC）测试与评估主任、总监察、法律顾问与国家安全局联络员；

- 特殊使命部门：白宫通信局和白宫情势支持参谋机构，负责与总司令进行联络；
- 共同业务部门：首席经济执行部、人力资源与安全部、采购部/国防信息技术合同签订办公室（DITCO）、战略计划与信息部；
- 策略业务部门：GIG 作战支持部、GIG 企业服务工程管理部 and GIG 运作部；
- 作战司令部野战办公室：DISA 中央司令部野战办公室、DISA 美国本土野战办公室、DISA 欧洲司令部野战办公室、DISA 联合部队司令部野战办公室、DISA 北方司令部野战办公室、DISA 太平洋司令部野战办公室、DISA 南方司令部野战办公室、DISA 特种作战司令部野战办公室、DISA 战略司令部野战办公室、DISA 运输司令部野战办公室、联合参谋支持中心（JSSC）、联合频谱中心（JSC）。

## 2 国防信息系统局的核心任务

国防信息系统局承担着许多核心任务，主要是提供高度集成、可互操作的 C4I 作战能力。核心任务领域主要有：通信、联合指挥与控制、作战支持计算、信息保障以及联合互操作能力支持，这些核心任务相辅相成、缺一不可，为美军提供了一个由通信网络、计算机、软件、数据库、应用及其他能力构成的无缝、保密、可靠的网络，以满足国防部在信息处理与传输方面的需求。核心业务包括采购、企业服务、网络运作、以网络为中心的企业服

务、频谱业务和 GIG 作战支持，后者包括计算服务、网络服务与应用支持。具体涉及：

- 全球国防部网络——话音、数据和视频:设计、建设并维护全球信息网格；
- 作战支持数据中心：美国本土 16 个，欧洲和太平洋各 1 个；
- 后勤、金融、运输、指挥与控制；
- 主要联合采购业务：以网络为中心的企业服务、网络赋能的指挥能力、GIG 带宽扩展、系统开发与支持以及全球指挥与控制（作战支援、报文传送）；
- 为联合特遣部队全球网络运作（GNO）提供兵力；
- 为每位作战指挥官配备国防信息系统局野战办公室；
- 对总统/白宫进行支持。

国防信息系统局旨在通过提供可联合互操作的系统、有保障的安全、可抗毁性和可用性，高质量确保美军在全球的信息优势。

国防信息系统局管理着 520 万美元的项目，受理 54000 个项目申请，签订 8200 个合同，为 1411 个武器系统提供支持。上述数据阐明了国防信息系统局向国防部任务领域提供巨大的信息处理与通信能力。可以看出，国防信息系统局需满足从前沿到维持基地的各任务团体的通信需求，以确保信息的可用性与安全性。

为了保持在全球的信息优势，美军一直致力于

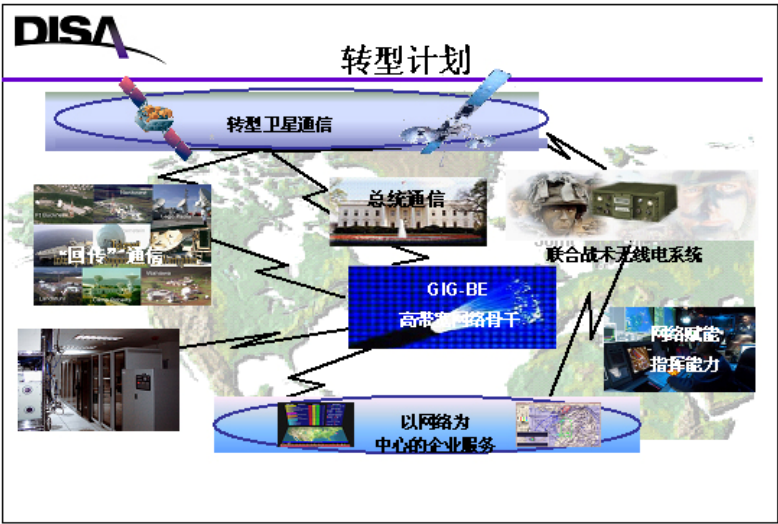
构建一个在全球范围内信息有效并按需获取的网络。信息受到基于能力的保护，使用户能以可靠方式连接、识别并存取所需信息。美军不论在哪里都可以部署并连接网络，拉取完成任务所需的信息，并得到有关他们所面临的任何威胁的及时而准确的信息。在维持基地和战术前沿之间建立无缝连接，以确保作战的灵活性。在这个世界中，美军能够自由地与盟军交换信息。使用的技术既灵活、自适应，又基于能力。此外，陆海空三军士兵都可拥有共享的态势感知。

### 3 国防信息系统局的网络中心发展目标与策略

目前，国防信息系统局致力于实现下列网络中心目标：转型通信、网络赋能指挥能力（NECC）、端到端系统工程和 IP 融合计划等。

#### 3.1 转型通信计划

转型通信计划包括：全球信息网格带宽扩展计划（GIG-BE）、网络为中心的企业服务（NCES）、联合战术无线电系统（JTRS）、转型卫星通信（TSAT），并由网络运作（NETOPS）将上述项目联系在一起。目前所有研究项目和研究计划都处于不同层次的研发过程。



上图说明了转型通信体系结构（TCA）全球互联的特性及其在建设和运行计划中所遵循的“多网络集成的网络”（Network of Networks）方法。正如所显示的那样，它包涵在网络管理“大伞”下运

行的国防部、情报界和国家航空航天局（NASA）系统的主要要素。

卫星网、机载网、部署的战术网和政府的地面基础设施将作为一个有效网络通过基于政策的管理

系统来运行。

在主要子系统内部的交换器和路由器的概念说明了各种形式的连接目前是如何构建的。具体的互联的点由于保密原因在上图中没有标明,但只要是使用了网际协议(IP)地址,就可以通过这个“多网络集成的网络”自动发送,利用的是一个“黑色核心”(保密空档)结构,根据“在任何地方连接任何人”的理论,在网络“边缘”管理加密。国防信息系统局管理的 GIG-BE 和国防部远程端口计划提供了一个关键的要素,可在系统间转换并翻译,以使这些系统无缝连接。

#### (1) GIG 带宽扩展计划

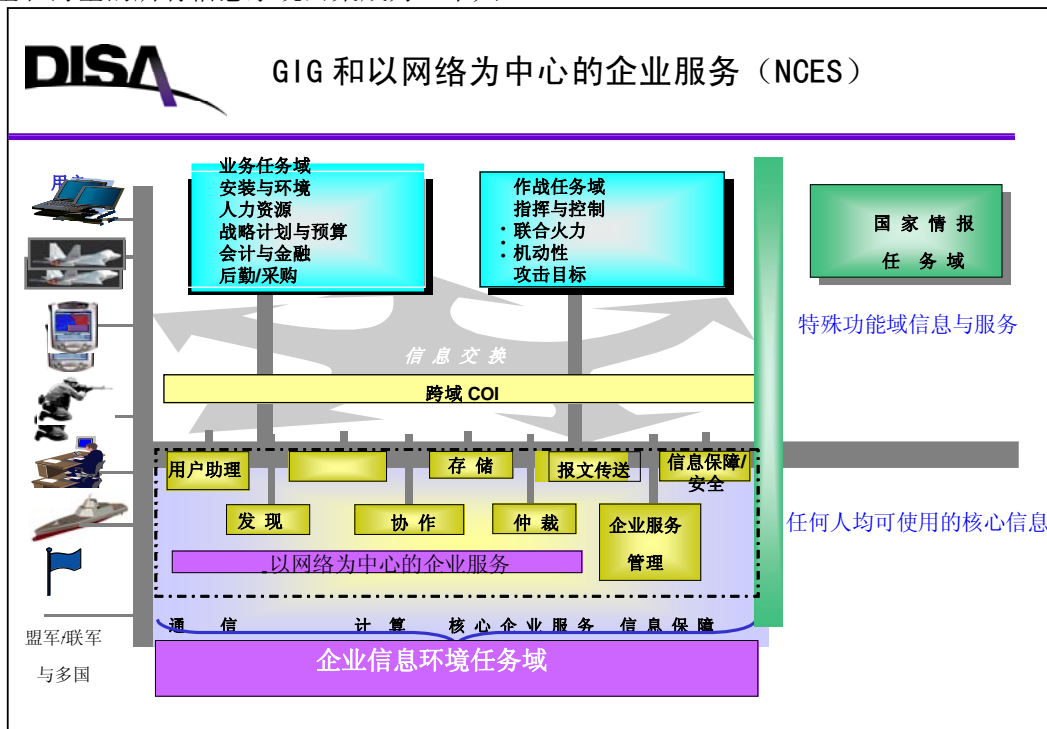
GIG 是网络中心战的实现基础,将美军天基、空基、陆基和海基的所有信息系统网集成为一个共

用的全球网,实时地为作战人员提供联合作战所必需的数据、应用软件和通信能力,以获取信息优势、决策优势和作战行动优势,支持网络中心战顺利实施,确保其军事战略目标的实现。

GIG 带宽扩展计划旨在建立一个全球性的安全高速的陆地光纤网,连接 100 个以上情报、指挥和关键作战站点,扩展带宽 1000 倍,大幅度提高 GIG 性能。

#### (2) 网络为中心的企业服务

“网络为中心的企业服务”计划将通过使用网络服务,使国防各机构可以使用以下九大核心功能:用户助理、应用、存储、报文传送、信息保障/安全、发现、协作、仲裁和企业服务管理。

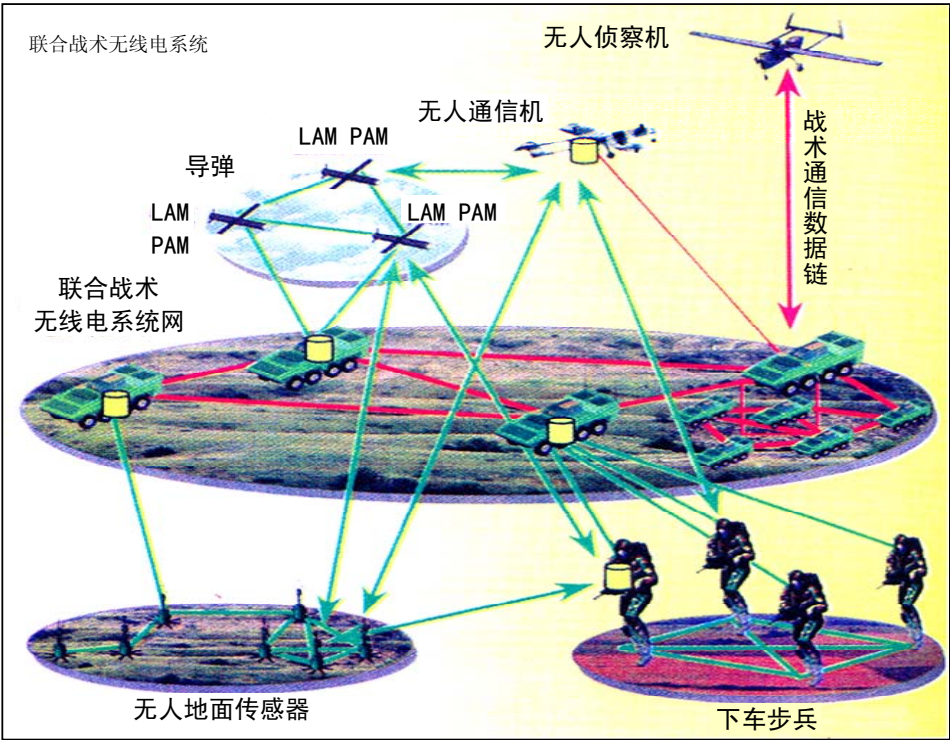


#### (3) 联合战术无线电系统 (JTRS)

联合战术无线电系统是多波段、多模式和软件可编程的三军通用战术无线电系统,能同时传输话音、数据和视频信号,具有定位、寻址、动态组网功能,并可与 43 种波形兼容的软件电台,计划用 25 万部取代三军现役的不同型号的 75 万部电台,以大幅度提高各军兵种互连互通能力和机动通信能力,预计在 2008~2010 财年具备初始作战能力。

#### (4) 转型卫星通信 (TSAT)

转型卫星通信计划发射转型通信卫星,将 IP 和激光引入卫星通信星座,支持机动和战术卫星用户使用网络通信。转型卫星通信由 6 颗卫星组成,卫星与地面用户之间采用射频传输,速率在 25~40Mbps 之间;卫星之间采用激光通信,速率为 20Gbps。



3.2 网络赋能指挥能力

为了进一步提高联合作战战场指挥的灵活性、安全性以及信息共享，美军全球指挥控制系统正向联合指挥控制（JC2）体系结构发展，预计到 2011

年前完成向联合指挥控制过渡。联合指挥控制系统代表美军下一代指挥控制能力，是美军转型建设的重点。而后 2014~2016 年将向网络赋能的指挥能力发展。

网络使能的指挥能力（NECC）

- 支持高作战节奏和决策的灵活的 C2 能力
- 基于以网络为中心的信息共享和网络服务

基于系统/计划的采购	基于能力的采购
多体系结构	面向服务的体系结构(SOA)
多采购结构/决策人员	单个的采购结构/里程碑决策机构
平台业务集成（COE）	利用核心企业服务（NCES）的 SOA 基础
确定的接口	实施国防部数据策略
预先定义的通用作战图像	用户定义的作战图

网络赋能的指挥能力是基于以网络为中心的信息共享和网络服务，是超越国家的、具有战略性的、互操作的全球指挥控制能力。

### 3.3 端到端系统工程

为实现基于效果的作战，美国防部各机构必须杜绝独立开发与管理各自的单个网络，以确保作战人员能够随时随地获得及时准确的信息。

上述目标的实现要求国防信息系统局将能力与业务推送到战术前沿。为此，国防信息系统局提出端到端系统工程的概念，端到端系统工程是一个通用策略与体系结构，它涉及到网络运作、配置控制和态势感知，每个要素都是从维持基地一直延伸到战术前沿。由企业信息环境（EIE）将数据置于网络并对信息进行管理，企业信息环境包括一系列确保数据准确的标准和规则。

### 3.4 IP融合计划

IPv6 标准是因特网的下一代网络层协议，并将改进端到端的安全性和服务质量，尤其是网络融合

参考文献（略）

#### 作者联系方式

通信地址：北京丰台区大成路 13 号

邮政编码：100039

联系电话：010-66820343

和移动通信。美国防部确定在 2008 财年完成 GIG 网络协议标准由 IPv4 向 IPv6 过渡，有效改进端对端安全和服务质量，提高网络覆盖和机动通信能力。国防信息系统局除了将其管理的网络升级到 IPv6 外，还将通过获得足以满足国防部近期和未来需求的地址资源，以及为促进互操作性和安全性，在企业级的基础上管理 IP 地址分配、登记和控制，在向 IPv6 转变中国防信息系统局起着重要作用。

为实现国防部网络中心战的设想，国防信息系统局的主旨是追求：可靠性，确保数据受到保护并且可用；传输，确保用户能够随时随地从维持基地到战术前沿都可存取信息；敏捷性，以因特网的速度获取和部署能力与服务。

针对上述需求，国防信息系统局将着力加快 IT 能力与业务的交付速度；加速推动从能力到边缘，即将企业服务推送到作战前沿；提升作战优势，加速提高作战效率和效能；在提供有效保护的同时确保信息共享。



# 面向服务的军事信息基础网络框架初探

赵为春 徐卫 马侃

**摘 要：**军事信息基础网络是一个面向军事信息业务应用的，集互联网和电信功能的综合集成型网络系统。该系统着眼于适应军事信息业务，以业务互联、互通实现数据高度共享为建设目标。本文从系统组成出发，描述了网络的基本功能，并提出了一个面向服务的基础网络的框架，最后对该框架下的业务服务质量保证措施进行了探讨。

**关键词：**军事信息服务中间件；集成网络平台

## 1 概述

以计算机、网络为核心的信息技术的发展，成为推动新军事变革发展的主要动力。军事信息系统之间的数据高度共享要求基础网络具有良好的互联、互通、对上层应用业务的高度适应性和良好的性能保证。因此军队信息化基础网络的建设设想应是能综合利用现有各种通信资源，架构一个广域的公用综合型网络平台，使它成为通用型军事综合信息业务应用的互联网和电信网。同时，作为军队信息化的支撑基础型网络应具备资源分配灵活、符合应用需求，集信息业务传输、交换、接入和多协议适配等应用于一体的，提供多种服务、扩展性好、易于维护、安全可靠的高性能网络，是信息技术、网络技术、设备产品和服务的综合集成系统。

## 2 网络的组成及功能

### 2.1 系统组成

面向服务的军事信息网络系统主要由两大实体部分集成：基础网络分系统和承载于网络分系统之上的业务应用分系统。基础网络分系统是承载所有业务的公共性接入、传输和交换平台。业务应用分系统涵盖各级、各类安全级别有限的军事信息业务部门。在两大实体中间，还有一个逻辑实体，即集成服务中间件，它由满足资源的预留、服务质量的要求，可完成各种网络集成功能的构件组成。如图 1 所示。这个逻辑实体是基础网络分系统的组成部分。

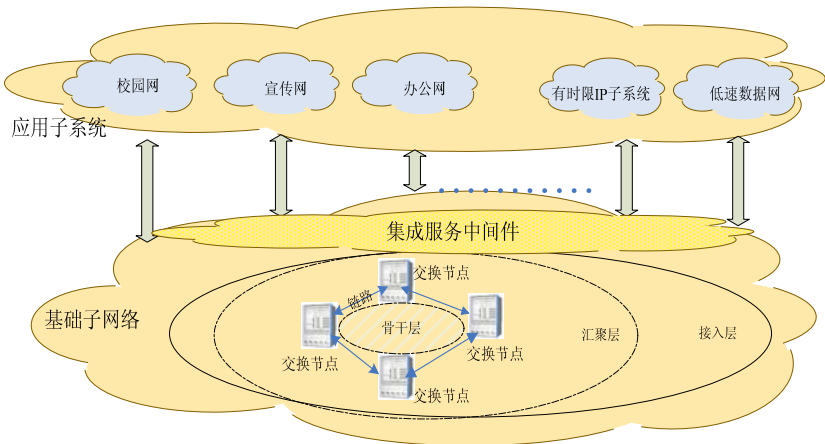


图 1 系统组成

### 2.2 基础网络的功能描述

基础网络的功能可概述为面向军队各种用户业

务需求、支持各种应用类型和适应各种应用环境集成定制的网络服务。它的主要实现方法是利用综合交换节点（如图 1 中所示）对各种接入技术的兼容

性，由驻留在综合交换节点中集成的应用中间件、服务定制和资源控制构件构成综合服务平台，提供给各个应用。如图 2 所示。这种框架下网络的功能主要体现在：① 通过节点设备中的服务定制模块提供新型的网络服务、实时/非实时业务、多点通信服务等服务的速率和业务的适配；② 通过资源控制模块对网络资源进行预留、对网络拥塞和流量以及网络 QOS 进行控制等；③ 通过由各种集成构件的组合而成的集成服务中间件，搭建适用于各种业务的统一应用服务平台；④ 通过通信和网络资源模块适配各种承载网络，为上层应用实体屏蔽异构物理层设备的具体细节。

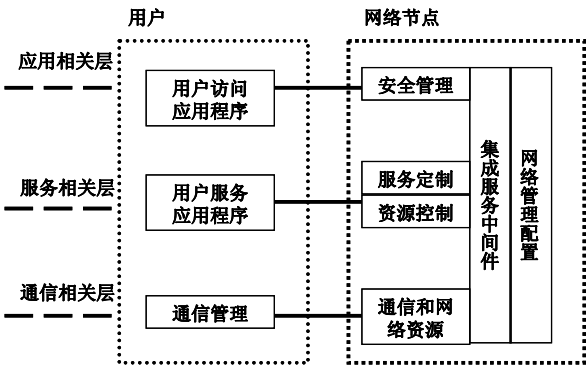


图 2 网络的功能框架

3 面向服务的基础网络框架

从上述对网络的功能描述可知，军队信息化基础网络是对设备功能、中间件服务和应用业务进行的综合集成。为适应多种业务的服务需求，传统的基于 OSI 七层协议网络模型严重割裂了用户需求与基础网络的关系，因此，我们提出一个更加合理的、适应性强、扩展能力好的基础网络框架。

3.1 面向服务的统一集成网络平台

军队应用需求多种多样，每个应用都是一个独立的分系统，网络设备、网络协议和网络软件各不相同；网络可利用的资源既包括军内计算机网，也包括军内电信网；既包括有线线路，又包括无线线路，网络的异构性越来越显著，主要表现为网络软硬件的多样性，服务平台和业务模型的多样性和不统一性。同时，应用对网络也提出了更高的要求，如网络既能兼顾各个业务部门自建的办公网络的路由功能，又能为有时限要求的 IP 数据应用系统提

供安全性、时效性和可靠性的保证；在保证 IP 业务服务的同时，又兼顾军队传统业务；在实现点到点通信的同时，满足点对多点传输的时延和抖动要求等。除此之外，还有其他可能的新业务、新要求，这些都不是传统的专用的服务平台和业务环境能提供的。为了能够在现有高度异构的通信基础设施上提供开放、稳定、高性能、可定制的服务，我们定义了面向服务的统一的集成网络平台，其体系层次如图 3 所示。

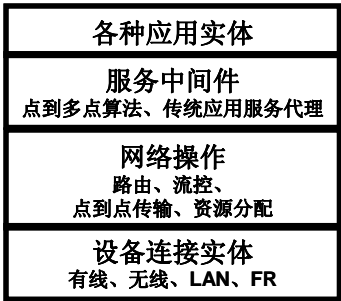


图 3 统一的集成网络平台层次结构

上图中每层代表的含义如下。

各种应用实体层提供面向应用的服务构件，它涉及军队信息化业务，包括网络业务中的所有文件传输服务、信息服务等应用；

服务中间件层提供端到端之间数据可靠传输、数据同步、多点算法和异构数据格式转换等应用服务代理模块，它是网络环境下为各种应用开发的服务模块的组合；

网络操作层提供端到端通信服务，包括提供跨越不同传输网的交换服务，构成虚拟专网服务，提供单播、多播和广播通信模式的互联网业务；

设备连接实体层提供不同物理位置之间的数据传输，包括有线、无线等传输手段，以及 OSI 模型二层以下的帧、信元的发送接收等。

3.1.1 网络集成应用平台的特点

- 1) 该集成框架通过服务中间件将各种应用实体和网络联系起来，结构清晰、层次分明；
- 2) 该集成平台体现了应用系统的功能特色，囊括了满足各种应用需求的基本功能；
- 3) 设备连接实体用于描述和规范网络资源的需求，它可以映射为任何物理的通信网络或传输网络，屏蔽了底层网络通信基础设施的异构性，实现了有线与无线资源的融合，实现了军事电信网络、计算机网络与网络应用的融合；



4) 该集成平台实现了各种异构的应用系统的集成。各个应用系统之间不直接发生相互调用关系和数据交换关系,从而降低了系统集成的复杂程度和协调难度。

### 3.1.2 业务需求向网络集成平台的功能映射

网络集成平台是由面向应用的网络功能构件组合而成,这些组合构件归纳如下。

#### (1) 对 IP 应用提供两种类型服务

基本网络服务:提供各个业务部门自建的办公网络,以 IP 等路由技术为主的互联网服务;

特定 IP 业务服务:提供独立于具体传输网络的、具有时间参数处理能力和网络安全能力的网络服务;

#### (2) 端到端多播服务

透明业务多播服务:为了保证数据业务的时延和时延抖动的相对固定,集成平台应尽量减少数据途经的节点,每个节点应减少对数据内容的分析,并通过服务中间件集成的路径算法,完成数据的复制、广播数据的分发及复用。

低速点到多点服务:提供低速数据接入和交换能力,网络功能构件中集成特定业务协议栈,完成本地数据业务的交换、数据包拆装、链路的建立、拆除和业务的流控;路由寻址等功能并通过增加相应处理模块的中间件功能,实现路由的聚合和拆分。

## 3.2 集成平台对服务(QoS)的保证

基础网络层对 QoS 保证的目的是为了进行合理的资源分配,它关心的是如何将用户的需求,如带宽和缓冲区等,映射到逻辑设备和端口,减少由于拥塞造成的网络时延和丢包。基础网络对资源的分配主要采用两种方式实现:资源预留和区分服务来分别满足 IP 应用的服务和端到端多播服务。军队信息化基础网络系统的 QoS 可针对不同的应用采用不同的方式实现。

资源预留方案中的服务模型:① 确保服务模型,它采用静态分配原则,根据每种用户的统计模

参考文献(略)

作者联系方式

通信地址:北京 2857 信箱空军装备研究院通信所二室

邮政编码:100085

联系电话:010-66918311

型估算和预测资源需求,并预先估算出应用流的峰值速率等参数,提供一个固定的、端到端的报文时延上界,并通过一个可定义的网络流量参数集,将应用层 QoS 映射到网络层 QoS,这个服务模型向用户提供了既确保时延、又确保带宽的数据传递服务。这种确保服务的模型特别适合于对时延及安全有要求的用户,是特定 IP 业务的服务保证模型;同时,为了满足网络可扩展性要求,即网络性能受其他应用用户或自身用户数量影响较小的要求,可采用动态流量分配的原则,以提供在网络高负载情况和低负载情况具有近似服务质量的服务。② 尽力而为的服务模型。它对所传的 IP 包同等待待,对时延和时延抖动要求不严格,因此它所提供的服务类型可以和目前普通 IP 用户所要求的基本应用很好地匹配。

区分服务方案基于优先权机制,可根据应用程序产生的数据流将业务分为有限几种流量类型,它通过用户所声称的流量类型来处理用户应用程序所产生的应用数据流,从而在不同的流量类型中提供一种逻辑上的服务区分。特别对于时延和时延抖动要求高实时业务,根据流量类型,采用不同业务分配不同优先级,同种业务采用固定排队算法,以保证时延和时延抖动的相对固定。所以它是端到端多播服务可采用的 QoS 保证方案。

## 4 结束语

军事信息化基础网络是一个综合型集成网络系统,如何充分利用各种通信线路和网络资源,发挥节点设备的技术优势和技术集成的潜力,使其在有限的资源环境下满足不同业务应用子系统的服务要求,是军事信息化基础网络系统在构架上需要着重考虑的问题。在此,本文只简单地探讨了系统框架性内容,还有一些其他重要问题,如安全能力及异构网络互联等未能涉及。这些内容将在以后的文章中进一步深入探讨。

# 信息资源动员建设发展策略探讨

周继文 韩伟 田忠

**摘要：**信息动员是国防动员的重要组成部分，是战争动员研究的新领域，是信息资源开发利用的重要方式，加强信息动员建设是做好军事斗争准备，打赢未来信息化战争的必然要求。该文从对信息动员的认识，建设任务，主要内容，信息动员机制，信息动员基础建设等几个方面探讨了加强信息动员建设的策略，为搞好我军信息动员建设提供了参考。

**关键词：**信息动员；信息资源；策略

信息动员，是指国家根据信息化战争需要，为建立并保持信息优势，调动、运用和控制经济、政治、科技和军事等各个领域里的信息资源所采取的 necessary 措施。当前应重点围绕我军信息动员建设中存在薄弱环节，转变思想观念，立足国情军情，借鉴外军经验，突出建设重点，理顺建设机制，充分利用现有优势和条件，抓紧做好各项信息动员建设。

## 1 转变思想观念，提高信息动员的地位和作用

现代战争是军事实力的较量，也是动员能力的较量，而信息动员能力则是维系信息时代战争的基础条件。随着信息作用的日益明显，世界各国都开始重视并加大了对高技术条件下局部战争中制信息权争夺的研究，其中对信息动员的研究更是提到了重要位置，并采取了相应的具体措施，使信息动员做到快速、有效、全面。尤其是近些年来发生的海湾战争、科索沃战争，伊拉克战争等使得各国对信息动员的重要性有了更为深刻的理解和认识，信息动员的地位和作用也日益突出出来，信息动员的特殊重要性受到了各国的高度重视。美国近几年举行的信息战演练，大都把提高信息动员能力，建立和保持信息优势作为主要课题，其他一些国家也都把信息动员纳入了国防动员领域，为未来战争中争夺信息优势奠定坚实的基础。

近几年来，我军信息动员工作已初露端倪，特别是在组织重大军事演习、应急救援、抢险救灾和维护社会稳定等任务中，动员了大量的民用信息网络资源，保证了“政令”、“军令”的顺畅传递。但我军信息动员工作整体上还没有取得突破性进展，

对信息动员建设的认识还不全面，存在着许多不足，在适应社会主义市场经济、适应高技术局部战争战场方面，还存在着一定的差距，无法适应未来信息化战争特别是军事斗争准备对信息资源的广泛需求。

信息资源在未来战争中居于主导资源地位，信息动员在现代国防动员建设中同样居于核心和主导地位。信息动员已经超越了通信网络资源动员的范畴，未来信息化战争对信息资源的需求领域将大为拓展，不仅仅包括通信网络资源，还包括信息网络、信息设备、信息技术、信息人才、信息科研、信息生产、信息安全防护等资源，动员工作十分复杂。因此，应积极转变思想观念，提高信息动员的地位作用，通过广泛深入地进行信息动员建设，将国家民用信息潜力转换为国防信息潜力，最大限度地积蓄战斗力，为赢得未来战争奠定基础。

## 2 围绕作战需求，明确信息动员建设基本任务

信息动员建设应围绕信息作战需求，以建立完善的信息动员机制、信息基础设施建设为重点，坚持“军民结合、平战结合”，加快信息动员机构、法规制度、指挥管理手段和信息专业队伍建设。信息动员建设的主要任务，包括以下几个方面。

一是进行信息动员理论研究。主要包括信息资源动员的概念，信息资源动员的产生与发展，信息资源动员的地位与作用，信息资源动员的经济基础及信息资源动员体系与方针等；通过理论研究解决信息动员工作的目标，方法，措施，手段，搞清信息动员的内容和范围，研究信息动员的特点和规律

以及需求和任务等。

二是健全信息动员组织机构，应按照有利于领导决策，有利于各部门协调，有利于开展工作，的利于形成整体合力的原则，建立权威高效的组织机构。通过改革和完善信息资源动员体制的指导方针和原则，信息资源动员体制的构造、功能及相互关系，优化信息动员组织机构。

三是建立完善信息动员法规制度，进行信息资源动员法规研究，通过研究信息资源动员法规体系的层次与结构，动员法规对信息资源动员的作用，信息资源动员法与其他法律的关系，信息资源动员子法等；根据市场经济环境的变化，坚持以国防法为依据，结合实际情况，制定切实可行的动员法规，保证动员工作的顺利开展，根据形势变化并不断调整。

四是建立信息动员信息系统。应根据信息动员领域宽，对象多，发展变化快，时效要求高，组织实施复杂的情况，建立高效灵活的信息动员信息系统，提高信息动员的时效。

五是搞好信息动员资源调查，应针对信息资源分布广，种类多，构成复杂的特点，采取统一组织，条块结合，归口统计等方法，对信息设施、信息网络、信息制造产业、信息科研机构、信息专业人才储备以及信息安全防护能力等信息资源进行调查。

六是搞好信息动员预案制定，应根据军事斗争准备和未来作战要求，结合各自任务实际，制定信息网络征用、信息技术动员、信息人才动员、信息物质动员等预案。

七是加强信息动员人才培养储备，应按照对信息设备熟练掌握的基本要求，加大信息专业人才培养力度，通过各种方式招收和培养具有信息管理、信息应用等特长的科技专业人才，采取一定的方式，加强信息动员在职人员的培训，建立一支以信息战分队为骨干，以专业技术分队为主体的后备力量队伍，不断提高信息动员能力。

### 3 着眼未来发展，切实理清信息动员主要内容

纵观人类战争历史的发展进程，我们可以清楚地看到，不同的社会资源构成不同的社会形态，不同社会形态有着不同的战争形态，而不同的战争形

态，其动员的领域、内容、重点和要求也有明显的区别。要加快信息动员建设步伐，就必须着眼未来发展需要，切实理清信息动员的主要内容，根据其内容特点，加快发展步伐。

从信息动员的定义看，信息动员涉及信息、信息系统和信息化装备等多个方面，按照不同的分类方式，既有对信息设备、信息技术、信息人才、信息产业生产、信息技术保障等，实施全面快速有效的动员。还有对民兵通信、信息战分队，邮电通信部门的技术设施和专业人员，公安队伍及其网络监控力量，国家安全部门有关力量，各科研院所有关信息科技人员及广大人民群众中的计算机、网络信息人员等动员。既有对民用通信网络资源的动员，又有对信息化战争所需要的广泛信息领域的其他信息资源动员等。

信息资源动员是信息动员的主体核心，它主要包括以下几个方面。一是信息网络动员，主要是根据战争需要，征用和调整民用信息网络，有效提高信息传输和交换的整体能力，动员具体内容主要依据平时对民用信息网络资源分布、容量、结构、技术体制和系统配置等掌握情况，按照征用方案，统一调度信息网络资源，保障部队作战需要。二是信息后备力量动员，主要是为适应战争需要，调整扩充军队及其他武装组织，实施信息力量补充。具体内容包括，征召信息预备役人员和有相关专业的适龄公民入伍，保障信息作战力量迅速扩编，并适时地进行信息兵员以及相应信息装备和信息物资的补充，对国家信息和其他部门信息人员的动员。组织信息技术人员收拢、教育培训、输送、扩充，加强军队信息作战力量。三是信息科技动员，指为保障战争需要，统一组织和调整通信技术研究机构、通信人员、通信设备、资料及成果所采取的紧急措施和活动。通过转变信息部门、研究人员的职能，实现为经济建设服务到为军事斗争服务的职能转变，使之从事战争所需的信息科学技术研究与开发。将具有军事用途的信息技术科学、应用技术应用于作战。四是信息物资动员，主要是采取相应的政策和措施，对社会拥有的信息物资重新配置。信息物资动员是一个国家进行通信动员的物质基础。信息物资资源包括信息装备器材及其附属设备、零配件等成品资源，生产制造各信息装备及其附属设备、零配件的原材料。具体内容包括统一调度使用库存装备，组织、动员企业生产作战急需的各类装

备器材和备件,协助军队抢修、维修各类设备器材。五是信息情报资源与安全动员,主要是通过与信息咨询部门合作,收集敌方,保护我方的社会政治、经济、科技、军事等各个方面的情报,满足作战需要。通过网络数据库、媒体、出版物等,收集敌对国家或地区的政治、经济、军事、教育等各方面信息,分类处理、去伪存真,为指挥员制定作战方案、下定决心提供参考和依据;同时向敌方散布假新闻、假信息,打乱敌方部署,使敌人难以达成正确的决策。六是无线电频率资源动员,主要包括掌握无线电频率使用和台站、设备配置等情况,拟定区域性无线电频率管制方案,实施无线电频率统一调配、集中管理,优先保证部队作战需要。

## 4 立足国情军情,制定信息动员建设目标规划

信息社会的资源分布表明,信息技术、信息人才、信息设备等优势永远存在于商业经济领域,而物美价廉、反应便捷的物资供应优势始终存在于社会大市场,使地方在信息网络建设、信息人才生长、信息传输和处理技术等领域远远优于部队。因此,从国情军情实际情况出发,在军事信息资源自身建设发展的基础上,提高民用信息资源转化为军用信息资源的能力,满足大规模战争对信息资源的需要,是信息动员建设的根本目标。

为实现信息动员建设的根本目标,应立足国情军情,制定具体的信息动员建设目标。应成立一个权威的动员组织机构,负责信息动员建设的领导和决策实施;应建立符合信息化战争、国防信息安全和军事斗争准备要求的独立信息动员体制;应建设包括信息动员机构、信息动员数据库、信息动员指挥控制系统等分系统的信息资源动员系统;应制定科学的信息资源动员计划和预案,正确组织信息动员实施;应构建科学合理的信息动员法规制度体系,确保信息动员的规范化;应建立一只具有较高信息动员素质的人才群体等。

为使信息资源动员工作更加具有科学性、计划性、灵活性和适应性,应综合研究分析国家信息资源潜力,提出合理的信息资源动员规划方案,更好地协调好军用信息资源和民用信息资源的关系。动员规划是整个信息资源动员系统的主要内容,通过分析、研究各类资源的具体情况,实现最终的信息

资源需求。动员规划主要包括根据各种战争模式要求进行信息资源建设和布局规划。根据现有的军用和民用信息资源的状况,提出现有实力规划方案。按照时间顺序,制定出短期、中期、长期的信息资源动员规划方案。为确保动员规划方案的实施,应综合考虑原材料、人才、科研基础、资金等多方面因素,统一制定国家信息资源动员总体建设及分布实施预案;信息战争条件下信息资源动员准备及战时实施的程序预案;信息资源动员对国家其他部门的要求预案;战时信息设备、人才征集调用预案;关键信息技术和设备的研制和购置预案;战时信息化武器生产和调拨预案等各种信息资源动员实施预案。

## 5 把握关键环节,建立健全信息动员建设机制

建立和完善信息动员体制是适应信息化战争的客观要求,是完成军事斗争准备的迫切要求,是提高信息动员能力的重要因素。

一是应建立信息动员机构。在海湾战争中,伊拉克没有信息动员机构,国家的信息防御意识十分淡薄,在美军信息攻击全面展开后,无法及时采取相应的信息防御措施,造成了十分沉痛的教训。由此可见,没有一个高度集中统一的信息动员机构,难以组织实施信息动员工作。因此,建立信息动员机构是信息动员建设的首要环节。信息动员机构既是信息动员法令的决策和执行机关,又是平时信息动员准备和战时信息动员的组织领导部门,是落实信息动员计划和措施的组织保证。信息动员涉及到上下纵横、军地内外各有关部门和单位,应尽快建立一个军队和地方共同参与决策、指挥的动员领导体制,明确职责分工,完善规章制度,确保沟通上下、协调军地。

二是制定完善信息动员法规。设立专职部门统一组织、协调,确保在征用民用信息资源时有法可依。信息动员工作能否顺利实施,不仅需要各级信息动员部门的共同努力和全社会的密切配合,而且需要完备的法律手段予以保障。目前,我国的国防动员法规尚不完善,信息动员法律法规建设更是一个薄弱环节,在许多问题上存在着无章可循、无法可依的局面,与未来信息化战争的要求很不适应。应在国防动员法基础上,分层次制定具有高度权威

的信息动员法规,明确各级、各部门、各类人员在信息动员中的职责、任务以及平时动员准备内容与方法、战时动员工作程序与要求,使信息动员工作实现从依靠行政手段为主到以法律法规调控为主的转变,为信息动员的准备和组织实施提供基本依据和可靠保证。

三是加强信息动员方法的研究,搞好信息动员试点,推广信息动员经验,根据民用信息资源的分布情况,拟制好军民结合信息保障预案并定期进行演练。针对野战信息系统(装备)与民用信息网技术体制的差异,以及使用民用信息系统面临的安全保密问题,加强相关标准接口和保密系统的研制,确保军民信息联合保障时的安全保密和互连互通。加强信息力量动员建设,应周密计划,精心实施,从信息人员到信息物资器材动员,以及信息技术科研和生产等统一精心筹划,科学安排,系统配套,详细造册,做到人员明,专业明,技术状况明,使用方案明,以便准确快速地组织实施信息动员。

## 6 借鉴外军经验,加强我军信息动员基础建设

近年来西方主要国家为了谋求信息优势,都将主要的人力、物力和财力投向信息领域。美国还抽调军队和地方科技信息方面的精兵强将,致力于先进信息技术的研制与开发,使动员机构美国信息系统中有近 80 %属于国防信息系统,美军的战略信息几乎所有传输电路都要依靠国家和商用电信公司提供,国家信息系统总部就设在国防信息系统局大楼内,国防信息局既负责军事信息系统,又参与国家信息系统管理,国防部三军武装部队及联邦政府其他部局的约 20 个信息系统,都在一起统一计划,分工建设,一旦战争需要,即可统一调用。

### 参考文献(略)

### 作者联系方式

通信地址:武汉市二七路 145 号二炮指挥学院三系通信教研室

邮政编码:430012

联系电话:027-85964878 85963841

目前,我国仅军事信息系统方面,就涉及到总部、各战区、军兵种和武警等各个系统;而民用信息系统方面除涉及中国电信、中国移动、中国卫星、中国联通、中国网络等集团通信外,还涉及铁路、公安、安全、交通、水利、石油、电力、银行等多个系统和部门。因此,要确保战时有效地利用这些民用信息系统,为国防信息系统提供支撑。应着眼信息动员工作项目杂、种类多的特点,建立和健全信息动员系统,发挥民用信息系统的优势,对信息网络资源、信息技术资源、信息人才资源、信息科研资源、信息生产资源、信息安全防护资源以及心理战资源等实施全面而协调的整体动员。应根据信息战对信息人才、设备等需求,立足现实,着眼发展,科学确立目标,按计划、分步骤抓好信息动员的基础设施建设,特别是需要尽快建设集数据管理、信息查询、信息处理、辅助决策、信息传输等功能为一体的国防动员信息网络系统。应坚持军民结合、平战结合的原则,充分利用科研成果的相互转化,拓宽民用高技术军事上应用的范围,提高信息武器装备的水平。要动员社会各方面的力量,加强信息技术的研究和开发利用,不断提高信息潜力的战备水平,为战时动员打下坚实基础。应立足最困难、最复杂的情况,本着军民兼容,就近就便,通用物资以地方储备为主,专用物资以军队储备为主的原则,采取国家、电信企业和军队相结合,成品储备与生产规划、生产能力、生产技术等动态储备相结合的方法,建立多元化、多层次、多渠道的通信装备器材储备体系。应特别重视国内紧缺的进口元器件、备板和备件的战略储备,以满足战时突击生产和维修需要。充分利用先进的信息和网络技术,建立通信装备器材储备管理系统,直接与被支援的单位联网,实施精确信息动员,提高信息动员的针对性和时效性。

## 第 2 部分

# 军事信息系统综合集成

# 军事电子信息系统综合集成技术

王积鹏

**摘 要：**本文讨论了军事电子信息系统综合集成技术的概念、内容和作用，分析了系统综合集成技术的理论与方法，阐述了军事电子信息系统综合集成技术的主要门类，包括：体系结构技术、系统集成设计技术、系统共性支撑技术、系统建模仿真技术、系统集成验证技术、系统工程技术。

**关键词：**军事电子信息系统；理论与方法；系统综合集成技术

## 1 引言

军事电子信息系统综合集成技术（本文简称“系统综合集成技术”）是在实践中逐步发展起来的跨学科、跨领域交叉融合的新兴技术，是军事电子信息系统研发中普遍适用的核心技术。随着不同领域的应用推进，系统综合集成技术自 20 世纪 90 年代以来取得了长足的发展。但是，至今学术界对系统综合集成技术并没有形成统一的认识，国内外对该项技术的研究探讨大多局限于某一领域，笔者尚未见到对其进行综述的文献。即使是该项技术的名称，也有很多不同的提法。

为了更好地把握军事电子信息系统发展的本质规律，本文基于理论研究和工程实践体会，尝试着对系统综合集成技术的概念、内涵、理论方法、涉及的主要技术门类进行了简要讨论，希望抛砖引玉，引起军内外对该项技术的深入研究。

## 2 系统综合集成技术的概念、内容与作用

1984 年美国专家 Roy W. Kuhnr 认为，综合集成是将多个单独的产品融为一个整体的过程和行动。1994 年美国军事系统工程专家 Jeffrey O. Grady 认为，综合集成是把复杂的大问题分解为多个相对较小的问题，由专家组解决这些较小的问题，并将这些解决问题的结果进行综合，用于解决原本的大问题的整个组织过程和行动。20 世纪 80 年代，钱学森等人在研究复杂系统问题时提出综合集成是处理“开放、复杂、巨系统”的思想方法，它以马克

思主义的实践论和认识论作为哲学基础，采用辩证法的思想将还原论与整体论相结合、定性描述与定量描述相结合、局部描述与整体描述相结合、确定性描述与不确定性描述相结合、系统分析与系统综合相结合，将逐渐形成了一门新的学科；运用综合集成思想所形成的系统理论、系统方法论和系统技术，均是综合集成思想在科学技术和方法论层次上的体现，而综合集成思想在工程实践中的应用，则产生了综合集成工程；综合集成思想、综合集成理论、综合集成方法、综合集成技术、综合集成工程，构成了综合集成体系；这一体系在科学技术向综合性、整体化方向发展，将会发挥重要作用。

对于军事电子信息系统而言，本文认为：系统综合集成技术是基于系统综合集成的理论、方法以及系统工程原理，将多个组成部分按照一定关系综合成具有特定功能、能力或使命的整体系统的行动和过程，是将系统构建为具有较高综合作战能力、实现信息资源最优配置的大型电子信息系统的一整套技术的总称。利用系统综合集成技术，可以将武器系统与人的聪明才智综合集成成为一个有机整体，实现各种作战要素的最佳结合，把军队各个电子信息系统整合成一个宏观有序、整体最优的大系统，形成远远大于系统简单相加的整体作战效能。

目前，系统综合集成技术主要服务于基于能力的综合集成、基于效果的综合集成等。其中，基于能力的综合集成主要采用“螺旋式过程模型”，如图 1 所示，美军在实施基于能力的网络中心战研究中，提出开发任务能力包（Mission Capability Packages, MCP）的方法，为信息系统与武器系统、作战力量的综合集成提供了有用的手段，并可以明确标识对系统的改进。基于效果（Effects



Based Operations, EBO) 的综合集成是近年来发展迅速的领域;美军在研究联合空中作战时,采用的基于效果的综合集成方法包括了基于效果的筹划、基于效果的执行、基于效果的评估等。但是,无论是基于能力的综合集成、还是基于效果的综合集成

措施,系统赖以发展的环境和条件都处于快速发展之中。为此,近年来世界主要军事强国都很重视建设系统综合集成的支持平台,提供军事电子信息系统发展所需的系统论证设计、系统综合集成、试验验证评估的技术支持手段。

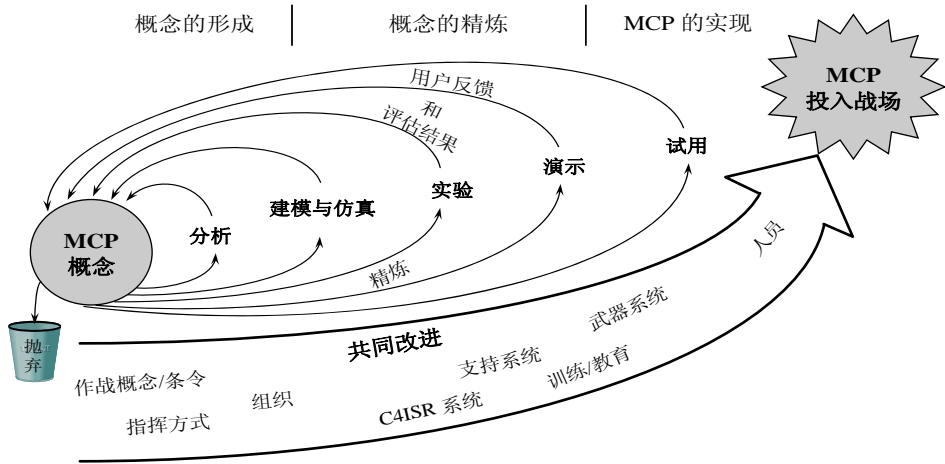


图1 任务能力包(MCP)的开发过程示意图

系统综合集成技术在军事电子信息系统建设中所起的作用主要体现在:可保证军事电子信息系统具有更高的作战效能和作战能力,使信息资源得到优化配置,提高系统的互操作性,保证系统应用软件具有较大的重用性,保证军事电子信息系统、武器和部队实现高度综合集成,全面提升信息时代的体系对抗能力。

3 系统综合集成的理论与方法

科学的理论方法是系统综合集成的灵魂和行动指南。现代系统科学可划分为哲学、基础科学、技术科学、工程技术四个层次,系统综合集成的理论与方法属于技术科学范畴,是直接工程实践活动紧密联系的技术科学,主要包括系统综合集成的理论基础、方法论基础、工程方法、过程模型等。其中,系统综合集成的工程方法是为完成工程目标,支持系统综合集成的规则、技术与工具的集合;而系统综合集成的方法论是进行系统综合集成探索的一般途径,它高于工程方法,是对工程方法使用的指导。在认识论层次上,方法和方法论是两个不同的范畴。目前,系统综合集成的理论基础、方法论基础、工程方法尚处于发展过程中,作为一门跨学科、跨领域交叉融合的技术科学,其来源一定是多方面的,将对军事电子信息系统的发展实践产生重

大影响。

系统综合集成的理论是系统综合集成的概念和原理的体系,它是在系统工程和系统理论的基础上,在新技术变革和新军事变革中发展起来的。系统综合集成的理论问题研究来自工程实践,其实质是“把工程实际中所用的许多设计原则加以整理与总结,使之成为理论,因而也就把工程实际的各个不同领域的共同性显示出来,而且也有力地说明一些基本概念的重大作用”。追本溯源,系统综合集成的理论基础可以归结为电子信息技术产生之后逐步发展起来的应用理论,包括控制论、运筹学、信息论、复杂适应性系统理论等与系统综合集成技术发展密切相关的理论。此外,系统论、相变论(主要研究平衡结构的形成与演化)、耗散结构论(主要研究非平衡相变与组织)、突变论(主要研究连续过程引起的不连续结果)、协同论(主要研究系统演化与自组织)、混沌论(主要研究确定性系统的内在随机性)、超循环论(主要研究在生命系统演化行为基础上的自组织理论)等也与系统综合集成技术发展有关。近年来,复杂适应性系统理论(Complex adaptive System, 简称CAS)的发展,对系统综合集成技术的发展产生了比较大的影响。CAS理论是1994年霍兰在美国新墨西哥州圣菲研究所(Santa Fe Institute, 简称SFI)成立10周年时正式提出的。它从系统演化规律的研究角度,提出



“适应性造就复杂性”的核心思想,认为适应性是产生系统复杂性的重要机制之一,但不完全排除还可能还有其他产生系统复杂性的机制和渠道。大量事实表明,由适应性产生的系统复杂性,即所谓的复杂适应性系统确实是一大类十分重要、非常常见的复杂系统。军事电子信息系统的主要特征都与这类系统相同。但是,无论从理论方面还是应用方面,包括软件工具支持方面,CAS理论都还处于初始阶段,还有许多问题要深入研究。学术界对CAS理论在军事电子信息系统这类开放复杂巨系统中的研究应用给予了很高的期望。

系统综合集成的方法论反映了研究和解决复杂系统工程问题的一般规律和模式,其基本特点是:研究方法强调整体性、技术应用强调综合性、管理决策强调科学性。应当指出,唯物辩证法是最重要的方法论,对立统一规律在系统系统集成工作中是强有力的武器,是研究方法论时应该学习、掌握、运用的基本手段。近半个世纪以来发展起来的霍尔和切克兰德的系统工程方法论、美国国防分析研究所提出的并行工程方法论、中国学者的物理—事理—人理系统方法论、反映信息化作战过程的OODA循环模型等方法论等对系统系统集成技术发展都起到了很大的作用。其中,霍尔和切克兰德的系统工程方法论是1968年美国贝尔电话公司工程师霍尔最早提出的,其核心内容是时间维、逻辑维、知识维的系统工程三维结构模型。英国学者切克兰德把霍尔提出的方法论称为硬系统方法论,他自己则在此基础上提出了软系统方法论。人们在运用霍尔和切克兰德的系统工程方法论时,作了许多演绎,逐渐丰富了该方法的有关内容。并行工程(concurrent engineering)是美国国防分析研究所在20世纪80年代提出、在计算机集成制造系统CIMS和系统工程中发展起来的工程方法论,已经成为美国国防部21世纪发展武器装备系统的基本管理指南;并行工程是对系统产品及相关过程,包括制造过程和支持过程,进行并行、一体化设计的一种系统化方法论,它力图使系统开发者从一开始就考虑系统全生命周期的所有因素,包括质量、成本、进度和用户需求。并行工程强调的四大要素是加速开发周期、提高系统质量、降低系统成本、提供优质服

务。法论是具有东方传统的系统方法论,它认为,在处理复杂系统问题时,既要考虑对象系统的物的方面(物理),又要考虑如何更好使用这些物的方面,即事的方面(事理),还要考虑由于认识问题、处理问题、实施管理与决策都离不开的人的方面(人理);把这三方面结合起来,利用人的理性思维的逻辑性和形象思维的综合性与创造性,去组织实践活动,以产生最大的效益和效率;任何复杂系统不仅涉及物、事、人,而且涉及它们三者之间动态、交互的过程,三个要素是不可分割的,它们共同构成了关于世界的知识,包括是什么、为什么、怎么做、谁去做,所有的要素都是不可或缺的。OODA(观察、判断、决策、行动)循环模型是1987年由美国空军上校John Boyd作为信息化作战的基本指挥控制模型提出来的。由于OODA循环模型系统地描述了信息化作战中,交战双方利用信息系统在物理域、信息域、认知域、意愿域的基本行为方式和周期循环过程,使得该模型成为研究信息化作战和信息系统综合集成的有效方法论基础;按照OODA循环模型,信息化作战首先从物理域开始行动,武装力量 and 信息系统能力都在这个领域中发挥作用;其次在信息领域,对抗双方将利用信息系统去观察收集数据;然后在认知域,对抗双方将采用人机结合的方式做出判断;最后在意愿域,对抗双方将在信息系统的支持下做出行动决策,并根据决策在物理域采取新一轮的行动。

系统综合集成的工程方法是为获取满足质量要求的信息系统产品,支持系统系统集成和维护过程的规则、技术和工具的集合。分析信息系统技术的发展历史,不难看出系统综合集成的工程方法大多脱胎于计算机软件开发工程方法,而且往往比计算机软件开发工程方法的成熟期滞后一个阶段。近年来,随着系统系统集成理念、系统集成技术的不断发展,系统综合集成的工程方法也不断地推陈出新,引领了系统系统集成方式的变革。目前,具备理论和技术支持、发展比较成功的系统系统集成工程方法主要有结构化方法、面向对象方法、基于构件方法、基于Agent方法。这些方法的共同特点是在形式化或非形式化的理论和技术支持下,利用自动化或半自动化的工具和环境,可为复杂系统集成的全过程提供支持,提升集成效率、系统质量、服务水平。四类方法是相互继承、逐步发展完善的。其中,前两种方法在信息系统工程和体系结

构技术中得到了普遍应用；后二种方法尚处于发展完善之中。军事电子信息系统在工程方法应用时，不仅要考虑一般信息系统开发所涉及的网络硬件、系统软件、基础信息等因素，更应在系统综合集成的设计和制造过程中，注重功能维、组织维、指挥级别维、空间维、时间维、使命维的综合集成问题。

系统综合集成的过程模型是跨越军事电子信息系统生存期的全部“过程、活动、任务”的结构框架，它能够清晰、直观地表达系统开发全过程要完成的主要活动和任务，可以作为军事电子信息系统研制建设的工作基础。系统综合集成过程模型应能支持系统全生命周期的开发、保障、组织过程，从应用规模和复杂程度以及管理、控制的模式来看，大致出现了三类过程模型：线性模型（linear model）、原型模型（prototyping model）和演化模型（evolutional model）。其中，线性模型包括瀑布模型和快速应用开发模型，一般应用于系统需求比较清晰的项目，我军常规武器装备研制大多采用这类模型。原型模型是对线性模型的改良，一般应用于通过原型试验后逐步确定系统发展模式的项目，我军战略武器装备研制大多采用这种模型。演化模型是对原型模型的进一步改进，一般应用于系统需求是在整个开发过程中逐步明晰的项目，强调系统综合集成是一个动态、渐进、分阶段发展完善的过程，比较适合军事电子信息系统这类项目的开发；演化模型的实现类型又包括增量模型、螺旋模型、双螺旋模型、基于构件的开发模型、喷泉模型、智能模型等。尽管从军事电子信息系统发展的角度，应该采用的系统综合集成过程模型是演化模型，比如可将系统发展分为科研综合集成阶段、装备综合集成阶段、战场综合集成阶段，分阶段解决军事电子信息系统的科研开发、装备建设、战场建设问题，逐步形成体系对抗优势能力。但是，对系统发展的各个具体阶段而言，所采用的系统综合集成过程模型还可以选择线性模型和原型模型。

## 4 系统综合集成技术的主要门类

系统综合集成技术适用于军事电子信息系统的“全系统、全寿命、全方位”，该项技术不仅需要理论和方法的指导，而且涉及到系统综合集成的产品整合技术、过程支持技术、环境应用技术，其中

发展较快、并被人们在工程实践中普遍采用的技术门类主要包括：体系结构技术、系统集成设计技术、系统共性支撑技术、系统建模仿真技术、系统集成验证技术、系统工程管理技术等。对系统综合集成技术范围与分类的讨论，学术界和工程界还没有形成统一的认识，有待进一步探讨。

### 4.1 体系结构技术

“体系结构”是指系统的组成结构及其相互关系，以及指导系统设计和发展的原则和指南。如同建筑设计一样，美军在进行  $C^4ISR$  系统建设时，要求先设计出体系的体系结构，并根据体系结构确定相应的投资和开发计划，指导系统的研制和建设。随着信息技术的广泛应用，美军已将体系结构技术的适用范围从  $C^4ISR$  领域扩展到国防部的各个任务领域，将其作为构建一体化武器装备体系、实现转型的重要技术手段，不断完善体系结构的开发规范，大力推进体系结构的开发进程，加快研制体系结构的开发工具，积极探索提高体系结构开发效率和质量的方法和手段。体系结构技术已经成为美军验证和评估新的作战概念、进行军事能力分析、制定投资决策、分析系统互操作性、拟制作战规划的重要手段和依据。

1990 年 IEEE STD 610.12 把体系结构（Architecture）定义为“系统或组成部分的组织结构”。1995 年美国国防部一体化体系结构专家组基于 IEEE STD 610.12 把体系结构定义为“组成部分的结构、它们的关系和自始至终指导设计和演进的原则和指南”； $C^4ISR$  体系结构和美国国防部体系结构均采纳这种定义。2000 年 IEEE STD 1472 提出“体系结构是概括系统的组成部分、它们相互之间的关系及对环境的关系和指导设计和演进的原则的基本组织”；这种定义补充了系统及各组成部分对环境的关系。军事电子信息系统体系结构一般是指系统组成部分的结构、它们相互之间的关系及对环境的关系和自始至终指导设计和演进的原则和指南。见图 2。

体系结构设计与系统设计是不同的。体系结构设计主要用于分析不同选择方案的差异、确定实际需求、进行采购决策、推进多个系统的综合集成，实现共同应用的目标。而系统设计的主要目的是用于分析系统的组成部分、构建系统或是当系统改进后搞清系统配置的变化。一般而言，体系结构设计

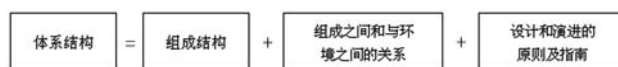


图2 军事电子信息系统体系结构定义示意图

可以分为系统级、巨系统级、机构级多个层次。系统级体系结构设计类似于一个建筑物的蓝图设计，巨系统级体系结构设计类似于一个建筑群的设计，而机构级的体系结构设计则类似于一个城市的规划。

从发展历程看，体系结构技术在  $C^4ISR$  领域的应用源于美军各个军种在  $C^4ISR$  系统开发中分别采用的信息系统结构化设计方法；美国国防部在各军种  $C^4ISR$  体系结构实践的基础上，研究推出了国防部体系结构的系列措施，采用结构化方法和面向对象方法，规范了国防部各个任务领域的系统综合集成工作。美国国防部先后发布了多个应用领域的体系结构框架版本，具有里程碑作用的包括：1996年10月发布的《 $C^4ISR$  体系结构框架》1.0版、2001年6月发布的《全球信息栅格体系结构框架》1.0版、2004年2月发布的《国防部体系结构框架》1.0版等。在制定体系结构过程中，美军非常重视开发体系结构所必需的指南和参考资源，在制定《 $C^4ISR$  体系结构框架》时，美军曾提供了9种参考文件，包括：核心体系结构数据模型（CADM）、国防数据字典系统（DDDS）、信息系统互操作等级（LISI）、通用联合任务清单（UJTL）、联合作战体系结构（JOA）、技术参考模型（TRM）、国防信息基础设施通用操作环境（DII COE）、共享数据环境（SHADE）、联合技术体系结构（JTA），并给出了这些文件对开发作战视图、系统视图和技术标准视图的支持关系；在后来制定《国防部体系结构框架》时，美军删去了联合作战体系结构（JOA），增加了一些新的参考文件，包括：GIG 体系结构、网络中心行动及作战参考模型、网络中心全域服务（NCES）、情报部门信息系统能力成熟路线图、北约互操作性程度等，这些参考文件对美军体系结构开发提供了必要的支持。

美军采取了一系列加快体系结构应用进程、推进系统综合集成的措施，包括：加强体系结构顶层设计和信息基础设施开发，加强观念转变和组织结构调整，加强信息技术体制研究和人才培养，为系统综合集成采用科学的理论方法提供了有力的保证。美国国防部推出的体系结构框架规定采用三种

视图的描述方法开发体系结构，即作战视图（OV）、系统视图（SV）、技术标准视图（TV），也就是描述任何体系的体系结构时，应从作战需求、系统总体方案、技术标准三个视角进行描述，把系统设计最关注的核心问题表述清楚；同时，在三个主要视图之上采用全视图（AV）描述军事电子信息系统体系结构的概况，确定军事电子信息系统体系结构的范围和来龙去脉。按照体系结构框架确定的基本原则和具体规则，体系结构开发的过程如图3所示，一般分为六步，在特殊情况下运用时允许剪裁。

在体系结构技术所必需的指南和参考资源中，信息系统互操作性技术占据了非常重要的位置，对军事电子信息系统综合集成是异常重要的。所谓互操作性，是系统、单位或部队与其他系统、单位或部队之间能互相提供和接收数据、信息、资料和服务，以及它们共同有效操作使用被交换的数据、信息、资料和服务的能力。信息技术和国家安全系统（NSS）的互操作性包括信息的的技术性交换和为完成任务所要求的信息交换的端对端作战有效性两个方面，这是上述定义的互操作性的特殊情况。信息系统互操作性的范围不限于信息系统之间，包括信息系统与其他系统、单位、部队直至决策人员和战斗员的互操作性能力。

军事电子信息系统的互操作性经历了互连互通、互操作、互依赖三个发展阶段。互连互通阶段的主要标志，是依托通信网络实现系统集成；互操作阶段的主要标志，是提出了系统互操作等级模型；互依赖阶段的主要标志，是依托公用信息基础设施实现系统的综合集成。目前，美军基于“网络中心化”理念所开发的军事信息系统，已经进入了互依赖发展阶段。

## 4.2 系统集成设计技术

系统集成设计的目标是从系统顶层提出研制项目综合集成以及嵌入现有系统的技术实现途径，确保系统建设能够按要求投入作战使用，形成实战能力。系统集成设计应侧重进行项目之间的网络互连、信息互通、业务互操作设计；重点对网络硬件

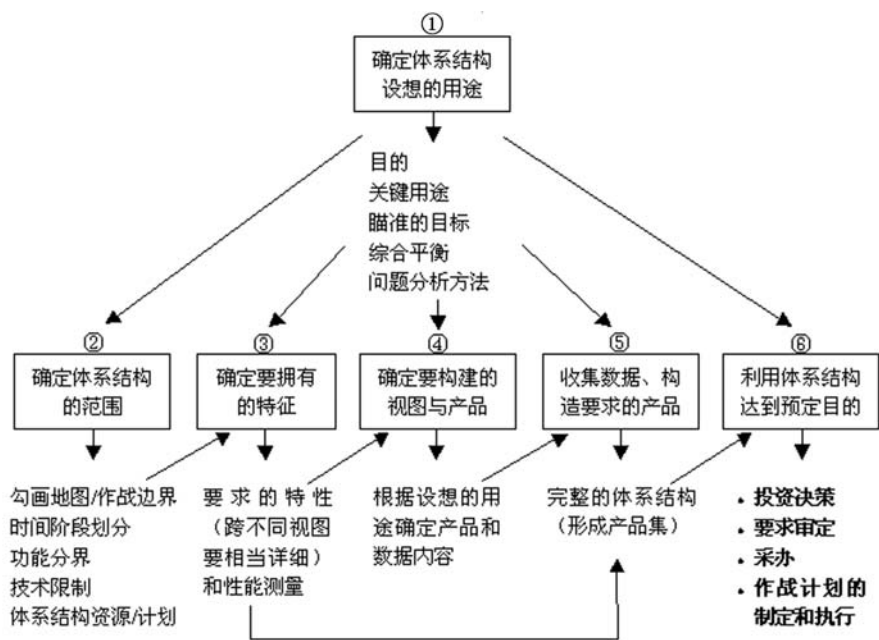


图3 建立体系结构的六个步骤

集成设计、软件系统集成设计、信息资源集成设计、系统互操作性设计给出技术实现方法。

网络硬件集成设计一般包括系统逻辑设计、系统物理设计、系统技术接口设计等内容。其中，系统逻辑设计，重点应明确组成项目之间的逻辑联结关系，将利用现有的国防通信网和新研的通信装备和设施，实现相互间的有效连接，满足各个系统逻辑连接的最低要求。系统物理设计的主要任务是提出系统项目之间、系统项目与现役系统其他项目之间，利用通信网络和计算机广域网络实施互连的技术方案；提出系统项目内部利用计算机局域网络进行连接的技术体制要求；同时，对系统计算机硬件平台的选型规定进行说明；重点论述各个项目应统一采用的技术体制和接入系统的技术途径。系统技术接口设计主要规定系统各个项目对外连接的技术接口设施，重点以通信系统为主线设计系统项目之间的接口关系，具体采用的接口标准应包括计算机网络标准和通信网络标准体系。

软件系统集成设计主要规范全系统的软件集成方案； 可通过推广使用通用信息处理平台，为提高系统互操作性奠定基础；提倡建立应用软件构件库，提高应用软件的开发效率和共享水平；逐步建立适用的数据模型和数据库，在部分领域内实现数据的共享和重用；推广采用软件工程化开发方法，提高应用软件开发和软件质量保证水平；建立军事电子信息系统的软件开发环境，为未来软件生产奠

定基础。为了提高系统项目的软件开发效率和可靠性，确保业务功能的互操作，从软件构架的角度，应将系统软件规范为平台软件、应用软件二个层次。其中，平台软件分为系统基础软件、应用支撑软件；应用软件分为通用应用软件（通用基础应用软件、通用业务处理软件）、专用应用软件（作战指挥类软件、模拟训练类软件、作战保障类软件、后勤装备类软件）。从发展的角度看，系统软件的具体分类不是一成不变的，将根据各类软件的成熟情况进行动态调整；例如，系统基础软件和应用支撑软件将根据发展不断地扩充完善；随着通用应用软件的不断成熟和商品化，部分通用应用软件将逐步演化为应用支撑软件，扩展平台软件域，提高系统的易获得性，改善系统的集成能力。

信息资源集成设计的主要任务是要界定系统的信息分类，提出系统项目信息交换的格式要求，为实现系统信息互通和部分共享创造条件。根据系统作战使用需求，系统各个项目之间交换的信息一般包括情报信息、指挥信息、保障信息三类；其传递的范围包括系统项目之间的信息交互关系、系统项目与其他项目之间的交互关系二类；按照敌、我、环境及业务保障内容可分为实时信息、情况通报、综合情报、综合战场态势、指挥控制等信息类型；按照表示方法可分为文、数、声、图、像等信息类型；按照信息交互手段，也可做多种划分。为了更好地服务于系统信息互通与共享，系统信息分类的

界定必须在数据建模的基础上,通过数据交换标准的制定来逐步深化。由于系统涉及面太广、信息种类繁多,国内要想建立统一的核心数据模型、提供相对完整的数据词典,在短期内是不可能实现的。正因为如此,系统研制过程中应以建立项目之间交换数据标准为重点开展系统信息设计工作,可在现有系统数据交换格式的基础上逐步完善,提供系统数据交换用的统一、权威性数据元素定义,建立系统数据交换用数据词典。

系统互操作性设计应给出综合性设计要求和实现方案,一般应提出系统互操作性等级要求,列出作战信息交互特征和特定功能集。为了提高系统的互操作性,可要求各个系统项目强制采用一体化的通信网络体制、统一的通用信息处理平台、一致的数据模型和健壮协调的信息安全体系等系统互操作性措施。尤其在信息系统安全方面,系统应针对安全威胁,对全局性的安全保密采取统一论证、统一

设计、统一开发和统一配置的策略,建立健壮的信息保密安全体系,提供信息传输、存储和处理过程中的多级安全保密功能,提供防假冒/防篡改/防窃取/防攻击功能,提供密钥自动管理和分发功能,提供身份识别、访问控制等功能,提供防黑客和病毒的能力。

### 4.3 系统共性支撑技术

系统共性支撑技术主要包括信息技术类、电磁兼容技术类、基础技术类的共性技术,规定了军事电子信息系统综合集成的主要技术体制,见图4。其中,信息技术类包括了信息处理和人机接口、信息传送、信息安全、信息建模和信息交换、软件工程化技术;电磁兼容技术类包括了系统电磁兼容、战场电磁频谱管理、防电磁信息泄漏技术;基础技术类包括了标准化、质量与可靠性等技术。

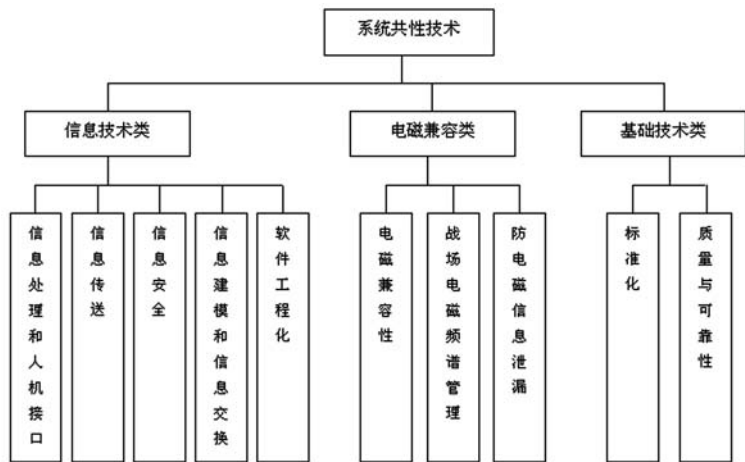


图4 系统共性支撑技术图

标准化技术的主要任务是说明系统标准化总体要求、目标、标准化系统;按照信息技术标准类、基础与工程专业标准类、系统装备标准类对系统标准体系进行了详细分划;规定系统标准化工作系统的组成和职责;描述了系统标准化的任务、工作内容、系统研制各阶段的标准化工作;对系统标准化工作系统的建立和管理、制定和选用标准的管理、宣贯标准的组织、监督检查的实施、系统标准化的协调作了论述;指出系统标准化的主要成果包括工程标准、技术文件、工具及资料。

质量与可靠性技术的主要任务是:从可靠性管理、可靠性技术、可靠性技术支撑三个方面描述系统质量与可靠性工作的基本内容;定义可靠性维修

性标准体系,说明系统选用的可靠性维修性标准、系统拟制定的可靠性维修性工程规范;简述系统质量与可靠性工作系统和管理工作;从可靠性工作项目的裁剪、可靠性工作的技术要点角度论述系统可靠性技术工作;分析系统可靠性技术支撑工作;规划系统可靠性总体工作计划;列出系统质量与可靠性工作应提交的软硬件产品。

软件工程化是采用工程化方法开发软件的一系列过程与活动。即,以数学和有关科学理论为依据,采用可定义、可量化、可管理的工程实践方法,实现软件开发过程的完全工程化。软件工程化涉及到理论与技术、标准与规范、组织与管理、工具与环境等四个方面,通常将其称为“软件工程化

四要素”。软件有一个孕育、诞生、成长、成熟、衰亡的生存过程，按 ISO/IEC 12207 国际标准的定义，软件生存期中所有活动可归纳为五个基本过程、八个保障过程、及四个组织过程。

信息处理和人机接口技术的主要任务是分析系统的战术技术要求，说明系统采用的“通用信息处理平台”技术方案和集成设计思路，描述系统模块设计，提出基于平台的系统集成服务与示范验证方案，论述系统人机接口的技术体系、风格指南体系、技术要求，列出系统选用的信息处理标准、人机接口标准和计算机网络标准。

信息建模和信息交换技术的主要任务是明确系统信息建模和信息交换的目的、基本概念、应用范围、具体背景，提出系统应强制性执行的功能模型、数据模型、系统数据定义、系统数据交换标准，列出系统信息建模和信息交换的各项标准。其中，信息建模和信息交换是为系统项目建设确定或提供信息建模、数据元素和信息交换最低限度的规范和标准；信息交换标准主要讨论系统之间或系统内部的不同任务域应用之间的信息交换，讨论与具体战术应用相关的信息交换标准。

信息传送技术的主要任务是提出系统通信网络体系要求，对固定通信系统、机动通信系统、军兵种通信网进行论证，描述系统网络互联与用户接入，提出系统嵌入现役系统的信息传送策略，说明计算机网络技术体制。

系统信息安全技术的主要任务是提出系统安全保密策略、安全保密服务配置以及安全保密设备使用建议。从技术发展过程看，系统信息安全技术已经经历了通信保密、信息安全、信息安全保障三个重要发展阶段。信息安全保障是“通过确保信息和信息系统的可用性、完整性、认证性、保密性和不可否认性来保护信息和信息系统，包括综合利用保护、检测和反应能力来恢复系统的功能”；它把“保护、检测、响应和恢复”（简称 PDRR）视为信息安全的四个动态环节，强调实施多层次防御，在整个信息基础设施的所有层面上实施安全政策、步骤、技术和机制，使得攻破一层或一类保护的攻击行为无法破坏整个信息基础设施；它从重视发展具体技术手段转向重视系统级的整体安全，强调“人、技术和运作”三大因素的相互作用，强调“风险管理”作为设计信息安全保障体系的指导思想和方法论，因此信息安全保障是信息安全的外

延，是全方位的概念，比信息安全更加全面。

系统电磁兼容性技术的主要任务是描述系统电磁兼容性管理的组织、职责、控制计划、工作目标，提出系统电磁兼容性标准剪裁原则、各种类型设备或分系统的电磁兼容性要求、系统项目的电磁兼容性要求，从检验责任、试验计划、具体试验、验收准则四个方面论述系统电磁兼容性试验要求。国外一般将电磁兼容性技术有关的内容归入“电磁环境效应”（Electromagnetic Environment Effect — E3），它是指电磁环境对军事力量、装备、武器和平台的工作能力施加的影响，主要研究在有限的空间、有限的时间、有限的频谱资源的条件下，各种用电设备或系统（广义还包括了武器平台和生物体）如何可以协调共存并不至于引起性能显著降低的一门科学。它几乎涉及电磁学科各个领域，包括 EMC、EMI、电磁缺陷分析（EMV）、电磁防护（EP）、电磁脉冲（EMP）、对军械的电磁辐射危害（HERO）、对燃料的电磁辐射危害（HERF）以及自然现象的影响，如闪电和静电干扰（P-Static）等。

战场电磁频谱管理技术的主要任务是描述战场电磁频谱管理的任务目标和总体工作要求，提出战场电磁频谱管理体系结构及应遵循的标准规范，详细论证系统战场电磁频谱管理系统方案。一般而言，系统战场电磁频谱管理应研究制定战场电磁频谱管理的标准规范和总体技术要求，提出战场实时电磁频谱管理的技术方案，组织开发战场电磁频谱管理的分析软件，进行电磁频谱的监视研究。应重点开发减轻干扰的技术，使同电磁环境的多种设备可同时使用；研究电磁频谱管理技术，开发出可以实际使用的战场电磁频谱分析管理软件，供系统项目使用；研究解决由于临近信道干扰而导致设备不能正常工作的方法。

防电磁信息泄漏技术的主要任务是对国内外防电磁信息泄漏技术进行全面分析，提出系统防电磁信息泄漏的具体战术技术要求；描述系统防电磁信息泄漏技术体系和具体支撑技术方案；列出系统防电磁信息泄漏的措施和研制的产品。

#### 4.4 系统建模仿真技术

系统建模仿真技术的根本目的是为系统顶层设计、综合集成、试验评估、培训研讨提供技术支撑手段，其主要任务包括三个方面：一是支持系统研

制建设，主要是提供系统论证和综合集成的手段；二是支持部队综合使用，主要是提供系统训练和分析评估的手段；三是支持系统采办管理，主要是提供系统全生命周期的协同服务。

系统建模仿真技术主要包括系统建模、系统仿真、仿真支撑环境三方面的内容。其中，仿真支撑环境主要针对复杂系统的不完整性，搭建实体、虚拟、仿真（PVS）混成结构的“系统环境”，为系统联试、系统评估、系统优化设计提供“舞台”。

系统建模仿真技术的主要基础是相似理论和可信性理论，目前对复杂的军事电子信息系统仿真而言，并没有普适的实用方法。支持系统建模仿真的技术框架发展，主要经历了分布交互仿真系统

（DIS）、聚合级仿真协议（ALS）、高层体系结构（HLA）等阶段，目前正在探索采用基于服务架构（SOA）、基于 Agent 等系统建模仿真技术途径。1995 年，美国国防部发布的《建模与仿真主计划》中提出的建模与仿真通用技术框架，包括高层体系结构（HLA）、使命空间概念模型（CMMS）、数据标准（DS）三个组成部分，为系统建模仿真提供了可供参考的标准体系。

系统建模仿真技术由于可以支持军事电子信息系统全生命周期的各种活动，目前受到了国内外的普遍重视，图 5 所给出的基于服务的军事电子信息系统仿真支撑环境的综合集成框架，就是一个典型的案例。

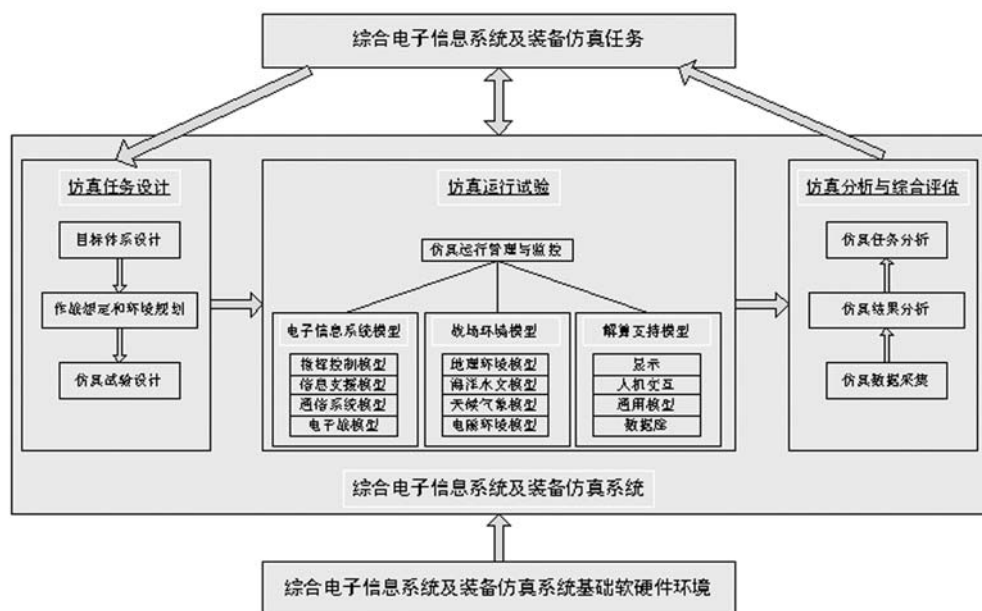


图 5 军事电子信息系统仿真支撑环境示意图

## 4.5 系统集成验证技术

军事电子信息系统的集成验证技术包括系统集成联试、系统测试与验收等工作。系统各组成项目在开发测试合格之后，通过集成联试对系统整体的适应性、正确性、互操作性和战术技术特性进行测试、试验和测试，直至达到全系统设计要求的过过程中所采用的技术称为系统集成验证技术。

系统集成联试是一个逐步进化的过程，是一种增量式系统综合试验方法，是促进系统各个项目研制工作、实现系统综合集成的关键，也是全面检验系统总体设计合理性、衡量系统总体工作的重要手段。系统联试旨在借助不断完善的系统研制成果，

在系统研制的关键阶段分别对系统总体技术体制的可行性、系统形成的综合能力、系统嵌入应用的技术途径逐步进行试验；通过联试，使用方和研制方可以在模拟的作战环境下弄清系统集成和新技术嵌入使用所带来的影响，以便于逐步对系统进行完善，保证系统最终投入部队实战使用，形成作战能力。系统联试作为一个增量式的过程，意味着军方使用部门与系统研制部门之间必须密切配合工作，才能将系统技术和先进的作战使用逐步融合为有机的整体。系统联试可依托系统仿真系统和集成试验床做支撑，联试规模可由小到大、由局部到整体逐步推进，重点应解决系统互与优化问题，可按照系统体制、系统功能、应用试验开展联试。为确保



系统联试工作的开展,可根据不同联试阶段的需要,成立不同级别的联试领导小组和系统联试指挥部,具体负责联试领导和协调工作。

系统测试和验收工作应分层次、分阶段开展。对系统交付部队使用的装备项目,除应按项目研制要求进行常规的测试和验收之外,应从全系统的角度对各个项目进行互联、互通、互操作测试和综合评估。对系统项目的测试验收工作一般包括常规测试验收、总体综合测试评估、系统嵌入使用综合验收三项内容。各个项目的常规测试验收一般应根据武器装备研制管理条例进行组织;各个项目的总体综合测试评估工作,应结合系统联试,在仿真系统的支持下,重点是从外部接口对系统项目的三互技术指标和主要技术体制进行测试;系统嵌入使用的综合验收工作,可结合系统联合演习和综合试验进行,通过对系统项目和现役系统的结合应用,重点对各个研制项目进行四类综合测试评估:接口和人机界面测试、软件系统的可靠性和安全机制测试、互连互通互操作能力测试、工程管理与交付成果综合评估。系统测试与验收要从整体上保证系统研制成果能够投入使用,滚动发展,形成一体化的信息系统装备体系。

从促进军事电子信息系统发展的角度看,应特别重视电子信息系统和武器系统的集成、新技术的嵌入集成工作。其中,电子信息系统和武器系统的集成,是建立传感器到武器系统环路、提高武器装备体系信息化作战效能的关键。新技术的嵌入集成工作,是增加和提高电子信息系统的作战能力,确保新技术、新体制、新系统嵌入原有系统,保证军事电子信息系统可持续发展、不断焕发新的功能和能力的关键。

#### 4.6 系统工程管理技术

系统工程既是一个技术过程,也是一个管理过程,是自然科学和社会科学相互交融的结果,它把工程技术和管技术结合成为一个统一的整体。系统工程管理技术作为系统系统集成技术的重要组成部分,是对系统工程进行综合管理控制的科学方法,是现代管理科学中发展很快的分支。其主要特点表现为三个方面:一是管理工作内容具有方法整体性、应用综合性的特点,涉及到军事电子信息系

统的“全系统、全寿命、全方位”;二是管理工作组织涉及面广,与军队领率机关和各个军兵种武器装备采办部门、有关部队用户、各个研制生产单位等方面都有关联;三是管理体制需适应军队编制体制的发展变化,制度上要求具有较高的规范化和科学化程度,应能服务于决策层、管理层、实施层等多个环节。

系统工程管理技术是指把系统军事需求转换为实际可用系统的过程中所开展的一系列管理工作。军事电子信息系统研制建设一般采用增量过程模型,系统研制建设是一个以系统总体设计和综合集成为主线的逐步进化的过程。在这个过程中,系统工程管理应抓住集成试验环节,建立适应系统采办体系的系统工程组织机制,规范项目合同管理、综合计划管理、技术状态管理、工程信息管理、标准化管理、质量与可靠性管理、软件开发与基础数据管理等工作。特别要不断完善综合计划管理、技术状态管理的手段和制度,不断提高军事电子信息系统研制工作的效率和科学性。

为了保证系统工程管理技术的有效性,军事电子信息系统应该分层次、分类型、有重点地开展系统工程管理工作。可根据军事电子信息系统采办管理体制的特点,按系统技术、共性技术、技术保障三个方面组织开展工作,全面推进整个系统的研制工作。

从发展的角度看,系统工程管理应吸收计划经济和市场经济二种体制的优点,逐步完善系统的采办管理;建立基于仿真采办(SBA)的科学管理模式;逐步完善工程管理技术;为解决公共操作环境、系统能力提升、复杂电磁环境等问题,支持“加强二头建设、加强能力建设、面向未来发展”的实施工作创造条件。其中,加强二头建设,就是要加强系统综合集成顶层设计和信息基础设施建设,规范和支持系统综合集成工作;加强能力建设,就是要从“基于威胁”的应对发展模式,尽快转向“基于能力和效果”的主动发展模式上,逐步提升系统的整体作战能力;面向未来发展,就是要适应信息技术的发展趋势,关注复杂电磁环境的相关问题,探索获取电磁优势、信息优势、体系对抗优势的途径,全面促进系统综合集成技术的发展。



## 参考文献

- [1] 钱学森等.一个科学新领域——开放的复杂巨系统及其方法论.北京.《自然杂志》1990 年 13 卷 1 期
- [2] 钱学森.再谈开放的复杂巨系统.北京.《模式识别与人工智能》1991 年第四卷第一期
- [3] Jeffrey O. Grady, System Integration, Boca Raton London New York Washington, D.C., CRC Press, 1994
- [4] Roy W. Kuhn, Implication of JTIDS/TADIL J onNAVY Aircraft Weapons Systems, AIAA/IEEE 6th Digital Avionics System Conference, 1984
- [5] Jeffrey O. Grady, System Integration, CRC Press London, NewYork, 1994
- [6] David S. Alberts, John J.Garstka, Richard E. Hayes, David A. Signori, Understanding Information Age Warfare, CCRP, August 2001
- [7] C4ISR Architecture Working Group. C4ISR Architecture Framework Version 2.0.18 December 1997
- [8] DoD Architecture Framework Working Group, DoD Architecture Framework, Version 1.0, .9 February 2004
- [9] Dr. Fatma Dandashi , DoD Architecture Framework Overview , October 2003 <http://www.opengroup.org/public/q403/dandashi.pdf>
- [10] Michael P. Bienvenu, Insub Shin, and Alexander H. Levis, C4ISR Architectures III:An Object-Oriented Approach for Architecture Design, Systems Engineering, Vol. 3, No. 4, Fall 2000.
- [11] US Air Force Accelerated Move Toward Effects-Based Operation, Defense International Review, 2003 October 1
- [12] Edward A. Smith, Effects-Based Operations-Appling Network Centric Warfare in P EACE, Crisis, and war, CCRP, November 2002
- [13] Paul K. Davis , Effects-Based Operations ( EBO ) : A Grand Challenge for the Analytical Community , 2001 <http://www.rand.org/pubs/monograph-reports/MR1477>
- [14] David S. Alberts, CCRP Overview, 1999 <http://www.dodccrp.org/events/1999-CCRP/alberts.ppt>
- [15] Maris McCrabb , Effects-Based Coalition Operations: Belief , Framing and Mechanism , 23 April 2002 <http://www.aiia.ed.ac.uk/project/coalition/KSCO/ksco-2002/pdf-parts/S-ksco-2002-paper-02-mccrabb.pdf>
- [16] Alessio Mosto, DoD Architecture Framework Overview, May 2004
- [17] 钱学森. 工程控制论. 北京: 科学出版社, 1958 年
- [18] 按照体系工程方法发展军事综合电子信息系统, 2006 年
- [19] 美国系统工程管理. 北京: 航空工业出版社, 1991 年
- [20] 现代集成制造系统概论. 北京: 清华大学出版社, 2004 年
- [21] 系统科学. 北京: 上海科技教育出版社, 2000 年
- [22] CIMS 的总体设计. 北京: 机械工业出版社, 1997 年
- [23] 系统工程引论. 北京: 清华大学出版社, 2004 年

## 作者联系方式

通信地址: 北京 2518 信箱

邮政编码: 100041

联系电话: 010-88797408

# 战区军事信息系统综合集成问题研究

张宏

**摘要:** 军事信息系统综合集成是一项长期复杂的系统工程,它涉及各部门之间协调、技术改造等诸多问题。其重点是解决系统互联互通的技术难题,建立顺畅的业务流程体系和良好的运行机制。近年来,我们以解决系统互联互通互操作和信息融合等问题为突破口,加强与相关科研单位协作,采取嵌入、组合、移植、开发、改造等方法,展开了军事信息系统综合集成的各项工作。

**关键词:** 信息系统; 综合集成; 问题研究

## 1 认清现状,紧贴实际,科学确立战区信息系统综合集成建设的目标任务

战区军事信息系统综合集成是一项时不我待的战略任务,也是一个长期复杂的系统工程。为此,应本着科学精神,务实态度,立足现实,着眼长远,紧贴战区信息化建设初级阶段的实际,科学确立战区军事信息系统的建设目标,扎实稳妥地做好打基础、管长远的工作。

### (1) 改造现有信息平台,夯实集成基础

目前,战区作战部队的信息系统通常包括指挥控制、预警探测、情报侦察、通信、电子对抗以及机要等其他分系统。由于这些系统的研发渠道不同,有的事先缺乏整体设计,易导致互不兼容,形成一个个“烟囱”,难以互联互通互操作,不但无法形成整体信息作战能力,而且也直接影响作战部队的信息化建设。因此,必须首先对这些系统进行全面整合。虽然,作为战区作战部队本身,无法从根本上解决这一问题,但作为系统的直接使用者,应从未来信息化作战特点以及对信息系统的要求,部队对信息系统组织运用的实践及其经验教训,指挥人员和技术人员对信息系统的操作使用体会及其改进意见等方面进行综合论证,提出科学合理的系统集成需求,供战区机关决策和科研部门制定集成改造方案时参考。同时,战区技术人员在积极配合上级进行系统集成改造的同时,还应发挥自身优势,积极开展力所能及的技术革新和小发明、小改造活动,以加快信息系统的综合集成改造进程。

### (2) 构建作战指挥系统,实现互联互通

当前,由于人员、装备编配等原因,各级都建

了许多“烟囱”,战区以下作战部队又不具备拆除重建这些“烟囱”的条件,只有发挥能动作用,在“大烟囱”上掏“洞”搭建“管道”,实现各“烟囱”间的互联互通。在实践攻关中,战区应指导部队按照实战要求,紧紧抓住建网络这个关键环节,规范技术体制、引进成熟技术、整合系统现有功能,通过在关键部位上实施重点改造,积极构建野战化网络平台,以促进现有作战系统的互联互通。一方面,可以对现有作战指挥信息系统进行综合改造。针对现有指挥控制系统传输速率低、组网手段少等问题,通过增加数字交换设备、跳频单元,改造通信网络节点交换设备等办法,提高各类设备互联互通的组网能力、数据通信能力、抗干扰能力;另一方面,可以引进成熟的移动通信系统。为解决不同兵种部队通信装备编配不统一、兼容性差,以及带宽窄、数据通信能力弱等问题,建成机动灵活的移动通信传输系统,通过接入军事信息系统,可以较好地实现指挥控制系统与作战要素之间的互联互通。

### (3) 整合情报侦察系统,适时获取信息

信息采集、处理、存储、共享是信息系统的关键。为改造整合部队情报侦察系统,应立足现有侦察段和实际能力,抓住关键,按照有限建设目标和本级需求,逐步进行系统集成。在实际探索中,应指导部队依托现有侦察手段和可能得到的加强,一体设计、分步建设,取得了初步效果。首先,可通过在现有侦察手段上加装各类信息技术,改造数字化接口,使其具备前端处理、格式报传输的功能,确保尽可能多地采集图形处理的有用信息;其次,可利用信息存储、显示和控制等技术,加强信息数据库建设,使信息能够按照实际需要,进行分门别

类、适时准确的存人、取出和综合运用,并利用图形处理系统功能,完成异地同步图形标绘,提高时效性;第三,可通过与各类信息系统的集成联通,实现战场信息和态势的实时传递与互通共享,为指挥员提供最为关注的战场综合态势。

#### (4) 统一集成标准规范,建设软硬平台

软硬平台的选型应满足信息化战场指挥控制系统互连、互通、互操作的实际需要,按体系结构进行。集成现有软硬件平台,实现各个应用系统的互联互通,是部队开展一体化作战训练和集约管理的物质基础。为规范当前部队业务管理系统和软件平台体制不统一、功能不融合、相互不兼容等问题。可指导试点部队在分析需求基础上,采取统一标准、整合资源等方法,依托现有军事信息系统,引入数据库格式标准和综合集成指挥训练软件,以作战指挥数据、动态信息资源和综合信息资源为重点,集成现有应用资源,构建包括数据库查询、综合信息处理、辅助决策和作战控制功能于一体的信息资源数据库;依托现有计算机网或局域网,利用成熟的仿真、多媒体、数字通信等技术,集成现有系统平台,统一整合各级作战值班、模拟训练、综合管理、后装保障等系统,优化整体功能,为部队信息化作战和训练奠定坚实基础。

## 2 抓住根本,渐进集成,积极探寻战区信息系统综合集成建设的方法路子

综合集成是衡量战区部队信息化建设成效的重要标志,是提高信息化条件下一体化作战能力的基本前提。实践中应本着“服务实战、提升效能”的原则,采取“从上至下整体设计、由下而上逐级集成”的方法,构建一个标准制式的作战指挥信息系统。

#### (1) 抓好应用软件功能集成,在提升作战效能上求突破

近年来,各级陆续配发了一些应用系统,逐步提升了战区作战部队的指挥、训练、保障和办公自动化水平。但由于上述系统研发的渠道、背景、时间和具体标准、协议、规范及基础平台的不同,导致相互不兼容,直接影响作战部队信息化建设进程,因此必须进行彻底整合。首先,应对现有的各类应用系统进行整理、分类,对每个软件从运行环境、系统的功能、应用前景以及在应用实践中暴露

出的问题和不足等方面作出客观评价。在此基础上,可提出对现有应用系统进行整合的方案和具体改进完善的建议,供战区机关决策和研发单位修改时参考。其次,应依靠自身力量,组成由指挥员、机关人员和技术人员组成的“三结合”攻关小组,对一些系统进行力所能及的修改完善,以推进作战部队的综合集成建设进程。

#### (2) 抓好单要素子系统集成,在优化信息融合上下功夫

单要素子系统集成是指将同类作战要素进行纵向间的一体化联结,是实现模块化集成和综合集成的重要前提。进行作战要素子系统集成,应该站在大系统的高度,依据全军信息化建设的有关规定,重点突破关键技术,采用统一体制、统一标准、统一接口,按照指挥控制、情报侦察、电子对抗等,分类别、成系统进行初级集成建设,逐步实现单类作战系统的上下联动、纵向贯通,实现其整体结构的优化,形成初级的信息化作战单元。通过整合信息资源,融合诸军兵种侦察情报、指挥控制和精确打击等作战信息,实现从传感器到指控系统到武器系统的无缝链接。

#### (3) 抓好战斗群模块化集成,在实现上下衔接上出成效

战斗群模块化集成,是在单类作战要素子系统集成基础上,按照作战力量编组小型化、多样化、集约化的要求,按照任务组群、模块链接、力量融合、效能提升的建设方法,对各类作战要素进行的功能整合。进行战斗群模块化集成,应根据作战任务的需要,组合成特种作战群、装甲突击群、火力打击群、网络攻击群、心理攻击群、综合保障群等不同的战斗模块,初步实现各类作战单元间的相互融合、整体联动,实现其作战效能的倍增。战斗群模块化集成,应坚持统筹规划,加强顶层设计,战略、战役、战术层次同步展开,试验、建设改革同步推进,作战平台集成、作战网络和作战要素集成同步实施,确保获取最大建设效益。

#### (4) 抓好作战体系综合集成,在增强协调发展上找对策

作战体系综合集成是军队信息化建设的根本目标和高级阶段,也是军队现代化的重要标志。进行作战体系综合集成建设,要按照一体化联合作战的要求,通过作战指挥信息系统,将指挥控制、作战力量、支援保障等要素进行一体化的“无缝”或相对“无缝”联接,达成全向、实时的互通、互联,

让“头脑”灵活控制“躯干”，进而达成指挥控制和作战行动的一体化，实现信息技术与指挥控制和综合保障的有机融合。作战体系综合集成后，实现作战指挥由“树状”结构向“网状”结构转型，作战形态由机械化的“捆绑”式协同向信息化的“融合”式联合跨越，较好地适应一体联合作战要求。在搞好作战体系综合集成的同时，应加强武器装备、综合保障和一体化训练等领域建设，加强一体化训练与理论创新，构建一体化联合作战体系，全面提高体系对抗能力。

### 3 深入研究，把握重点，加速推动战区指控系统综合集成建设的对策建议

综合集成是一项复杂的系统工程，也是一个不断深化的长期过程。随着技术的发展和军事需求的变化，综合集成在解决现役装备遗留问题的同时，又会对未来的装备体系建设不断提出新的要求。因此，在开展综合集成工作时，应坚持科学发展观，正确处理好各种关系，确保综合集成方向的正确性、科学性。

#### （1）应注重搞好整体设计

综合集成是战区作战部队信息化建设的核心思想。作战部队的综合集成建设，一定要有整体意识、联合意识，在全军顶层设计指导下，按照统一的技术体制去思考、去设计、去建设，搞好本单位内部的小的顶层设计，从互联互通的角度，提高建设效益。要坚决防止和克服建设的系统不兼容、标准不统一、功能不规范，重树“烟囱”等现象。应根据信息系统综合集成的特点规律和建设需要，全面整合优化现有职能部门，克服机构重叠，减少任务交叉，理顺集成关系，在战区信息化建设领导机构的组织指导下，各负其责，稳步、高效地推动战区信息系统综合集成建设。

#### （2）应注重搞好需求分析

科学合理地确定符合部队实际的有限目标和基本需求，是搞好整体设计、提高建设效益的关键所在。一方面，要抓住最核心的要素。比如，在分析指挥决策系统建设需求时，抓住指挥员最关心、对作战指挥最重要的战场态势这一关键因素，作为系

统设计的第一需要和基本需求。在实现这个功能的基础上，考虑相关局部信息和作战资料的采集传输，帮助指挥员分析判断情况，而不必在指挥员没有时间关注的动态图像传输上费钱费力；另一方面，要寻找最便捷的途径。比如，在分析情报传输系统建设需求时，可采取就地开矿选金子的方法，利用简易信息技术，把前端侦察单元获取的情报信息，统一处理后传输上报，再经过情报中心的整理融合，就可变为指挥员直接利用的作战信息。

#### （3）应注重搞好军民结合

当前，作战部队信息化建设，一方面需要技术创新攻关，更需要把指挥人员和技术人员紧密结合起来，使建设需求和技术优势相统一，最大限度地挖掘技术潜能，提高建设效益；另一方面，由于信息技术的快速发展，我国民用信息技术已缩小了与西方强国的差距，有些甚至达到了世界领先水平，为军队信息化发展提供了坚实的技术平台。因此，可指导试点部队积极利用成熟的民用技术，立足实际，土洋结合，军民结合，积极借鉴，按照统一的技术体制，经过相应的技术改造和完善加工，直接运用到部队的武器装备改造、综合集成建设上来，积极探索由“军转民”到“民转军”这条新的发展路子。

#### （4）应注重搞好攻坚克难

战区作战部队军事信息系统综合集成，应坚持“有所为，有所不为”的原则，以搞好指挥指控装备建设为重点，促进军事信息系统综合集成建设的快速发展。当前，首先应加强一体化联合作战指挥信息平台建设，实现信息综合处理、联合指挥作业、联合数据共享等功能；其次，应加强战术互联网建设，提高作战信息传输能力和各作战要素对战场信息的共享能力，实现作战部队“三军通”、“动中通”、“扰中通”；第三，应加强数据链体系建设，实现指挥控制系统、预警探测系统、武器系统间的无缝链接和信息实时传输，满足联合作战精确指挥和武器精确引导控制的需要；最后，应加强天基信息系统建设，为分布于陆海空天的各类传感器、武器平台、指挥控制系统提供有效的信息传输手段。通过攻坚克难，带动战区军事信息系统综合集成的整体跃升。

参考文献（略）

作者联系方式

通信地址：北京市石景山区八大处甲1号104信箱

邮政编码：100041

联系电话：010-66399874

# 利用建模与模拟支持系统综合的试验评估

施振明

**摘 要:** 本文根据利用建模与模拟对系统综合进行试验评估的活动过程,系统地介绍了各相关活动的主要内容,并详细地阐述了试验环境中主要成员的建模方法。

**关键词:** 建模; 系统综合; 试验评估

## 1 引言

随着许多新的信息系统装备的开发和使用以及各种支持联合作战设想的提出,系统与系统的综合越来越成为信息系统发展及其作战支持能力提高的关键。

为了弄清楚联合作战需求以及系统与系统综合后满足这些需求的潜在能力,辅助综合系统的螺旋

型开发,必须对其进行各种试验和评估,如果依靠来自不同军种的各类系统在战场环境下一起运作来完成此项任务,其花费将是惊人的,而且一般是行不通的,实际上只能依靠建模与模拟。

利用建模与模拟对信息系统的综合进行试验评估的过程如图1所示。

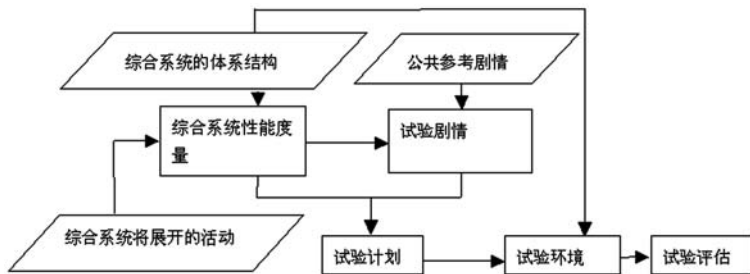


图1 利用建模与模拟对信息系统综合作试验评估过程图

## 2 综合系统体系结构及其活动

综合系统体系结构是为支持某种联合作战设想,将系统与系统进行综合,确保系统间实现互操作,从而达到改进作战能力的这样一类“系统的系统”的设计基础。它往往是根据一个确定的范围和一个特定的角度开发的。综合系统的体系结构完全是以任务领域和作战过程为基础的,清晰地描述了系统与系统间如何联系和协作,以完成相关的各类作战任务。例如,当将武装侦察直升机与地面C<sup>4</sup>ISR系统综合时,其任务就有可能包括武装侦察、精确火力打击、护送空中兵力、支援指挥控制等。为了应对这些作战任务,综合系统就要展开各种不同的活动,从而对它提出一批能力需求。像在综合防空反导系统中,其能力需求有四个方面,即

单集成空中画面(SIAP)、战斗识别(CID)、综合火力控制(IFC)和自动战场管理辅助(ABMA)。因此,了解综合系统的体系结构,认真分析系统将要展开的各种活动及其能力需求,是确定综合系统试验目标,进而完成整个试验评估任务的基础。

## 3 综合系统性能度量

综合系统性能度量被用于客观地评估综合后的系统在展开各种活动时实现能力需求的状况。它使我们了解现在的系统综合作(或综合设想)已能达到什么样的能力状况,在哪些方面还需要改进,以及改进后将达到的能力。综合系统性能度量与系统支持联合作战的构想,将展开的活动及需要实现的能力紧密相关。它往往通过一种广泛范围的作战

效能度量、任务能力级的综合系统品质度量和参与综合的有关系统的性能度量来体现。确定能定量，能测试的作战效能、品质和性能是对综合系统进行试验评估的关键之一。建立一套公共的专用术语，将各级度量收敛到一个标准化的大家赞同的度量集上是一项至关重要的基础工作，需要有关军事部门和工业部门的共同努力。特别是军事部门要起主导作用。例如，美军的联合需求监督委员会（JROC）以战区防空反导和战斗识别顶层需求文件（TAMD CID CRD）中关键性能参数（KPP）的方式为综合防空反导系统单集成空中画面（SIAP）能力、战斗识别（CID）能力的度量制定指导意见。美军方专家和工业部门专家相结合的联合 SIAP 系统工程机构（JSSEO）则为品质及相应的度量方法提出数学表达式。美军的联合战区防空反导机构（JTAMDO）进行综合系统的作战效能度量，支持引出顶层需求文件关键性能参数的具体阈值和目标。品质度量是综合系统性能度量的关键，因为它集中地体现了综合后的系统本身的能力，有效的构筑了从底层的性能到上层的作战效能的桥梁。美军对综合防空反导系统单集成空中画面（SIAP）能力的品质度量规定了五点，即完整性、明晰性、连续性、精确性和共用性。

4 公共参考剧情与试验剧情

为了使综合系统的试验评估紧密结合实际应用背景，需要研究确定其潜在作战应用区域的一批公共参考剧情作为试验的基本背景。这些剧情描述了

红蓝双方在具有重大时间分段的战役中动态交互的情景，其中的威胁特征是根据最近的情报评估作出的，并不断的进行周期性的修正。这些公共基准剧情应是在军事计划指导下制定的，并且得到相关军事指挥机构和人员的认可。

试验剧情是针对综合系统试验评估的目标做各种具体试验评估时所用的剧情。它是公共参考剧情中选择一个较完整的部分或仅仅抽取其中的一个局部或侧面作为基础，进行了有目的的修改后形成的。因此它能更好的为某种试验评估作业服务。

5 试验计划

试验计划包括数据管理与分析计划，它规定为实现试验评估目标所需采集和分析的数据以及做这项工作所要用到的详细的仪器设备名录。试验计划还包括了试验过程的简介、做各种偏离试验的方法以及试验所用的剧情。试验计划也提出了详细的试验方案以及试验参与者们的角色和责任。整套试验计划形成了开发试验环境、进行综合系统试验评估的基础。

6 试验环境

根据试验计划和综合系统的体系结构就可以构筑试验环境。当前试验环境的开发和应用通常按照联邦开发和执行过程（FEDEP）来进行，如图 2 所示。



图 2 联邦开发和执行过程图

综合系统体系结构和试验计划已把图 2 中的用户问题空间描述清楚了，而图 2 中的联邦运行应用阶段实际上就是对综合系统进行试验评估工作。因此，试验环境的构筑对应的只是图 2 中的开发联邦阶段，也就是做好第 3、4、5 步。

设计开发联邦的核心问题是仿真环境中各类成

员的建模以及它们的集成问题。建模采用的方法及模拟粒度的粗细，都与具体的试验评估目标有关。模型中有的采用硬件在环中的模拟设备，有的采用人在环中的模拟设备，有的则采用纯数学方法的模型。即使是纯数学方法，也还分了许多不同的粒度等级。

硬件在环中的模拟设备通过使用实际系统的部分真实硬件和软件达到模拟的高逼真度。特有的硬件和软件组件的使用，使得试验人员能很好地控制和重复试验，并且做出比较可靠的前后对比。但由于这类模型花费较大，在试验中不可能普遍使用，所以只能在特殊需要的场合才采用。例如，美军利用 Link-16 数据链将多类系统和武器平台综合起来形成单集成空中画面（SIAP）的试验环境中，就有一种舰载预警机 E2C 的硬件在环中的模拟设备。其中 E2C 平台上的雷达、传感器和数据链设备用数学方法模拟，E2C 上的任务计算机则使用实际装备的计算机及其软件。这一硬件在环中的模拟设备对于精细地模拟分析时间同步上的偏移和数据注册上的偏移对综合系统 SIAP 能力的影响起了很大的作用。

人在环中的模拟设备对于有效的模拟出操作员与系统交互的影响、人的决策的影响特别重要。这种影响是评估综合系统实际应用中的作战效能的重大因素。然而人在环中活动就像硬件在环中活动一样，能力上是有限的。虽然硬件在环中能较好地进行控制和重复试验，并且能进行可信的前后比较；但人在环中活动的重复能力实现上却很困难，尤其当试图获得统计上有意义的运行次数时。当前国外应用了较多人在环中模拟设施的是支持美军未来战斗系统（FCS）开发与综合集成的试验环境。该环境中大量应用了一类能重构的桌面模拟设备。这些基于便宜的 PC 机构筑的模拟器，在实际试验中每

台前安置了一个作战人员，并为他们提供了一套灵活模拟的显示和职能控制设施，使他们在试验中能像在实际车辆中的驾驶员、指挥员、枪炮手战斗中所做的那样。此外，澳大利亚的用于试验武装侦察直升机与地面 C4ISR 综合问题的综合环境，则用了直升机座舱模拟器进行人在环中的模拟试验。这个模拟器构造得能使参与试验的飞行人员感觉在穿空飞行，并能和实际的战斗空间进行交互。

纯数学方法的模型也称结构化模型，它的最大好处是可塑性强，可控制、可重复。它既能代表已有的系统，又能代表潜在的系统甚至概念系统，在试验环境中可反复多次运行，一致性好。然而，纯数学方法模型虽在表现大量系统和可重复性上十分强大，但在精确度上却较有限。尽管如此，随着模型粒度的变细，复杂度的提高，其精确度往往也能满足试验要求。而且在许多试验评估活动中，一些较粗粒度的模型也已经够用了。在美国海军的联合指挥控制试验中，为研究陆上攻击武器系统如何与海军的各种传感器，情报中心等系统的综合问题，广泛应用了海军模拟系统（NSS）中的传感器模型、通信模型、情报中心数据融合模型等。这些模型都是一些不同粒度的纯数学方法的模型。美国海军模拟系统中与传感器有关的模型分三级粒度，如表 1 所示；与通信有关的模型分四级粒度，如表 2 所示；与数据融合有关的模型也分四级粒度，如表 3 所示。

表 1 传感器有关模型的三级粒度

粒度	模型	描 述
粗	简单参数模型	传感器由一个小的参数集表示，如检测距离、监视周期、能监测的脆弱性、检测概率、分类识别能力，每次监视的战斗毁伤评估能力等
细	详细参数模型	传感器由一个较详细的参数集表示，如它们还包括以高度、方位、仰角所表明的限制、目标的 RCS、扫描速度、视线限制、由地点、环境、地形等引起的性能改变等
很细	基于物理学的模型	传感器在传播物理学的详细程度上被模拟，需要传感器、目标和环境的广泛数据做支持，常常需要做大量计算，模拟中常有延时

表 2 通信有关模型的四级粒度

粒度	模型	描 述
很粗	拥有随机时延的有把握的通信模型	所有的通信都被假定为按通信计划进行的，用户指定时延分布
粗	拥有简单限制的无把握的通信模型	所有的通信都被假定为按通信系统计划进行的，用户指定时延分布，但加上了一些简单的限制，如视距通信的限制、频率一致性上的限制等
细	规程级通信模型	与特定的通信系统相联系的规程被模拟，如 JTIDS 的时隙块分派及逻辑、有关战术接收设备的存取时隙分派及逻辑等
很细	基于物理学的通信模型	通信在传播物理学的详细程度上被模拟，需要通信系统及环境的广泛数据做支持并做细致的计算，模拟中常有延时

表 3 数据融合有关模拟的四级粒度

粒度	模型	描 述
很粗	“磨碎的真实”模型	战术图象包含所有我方、敌方、中立方平台的“磨碎的真实”的位置、速度、类型、识别、数量和战斗毁伤评估数据，对敌方兵力或友方兵力或所有兵力用此模型时，相应的兵力无需传感器模拟
粗	“具有外推的完美地关联”模型	所有的观察报告被假定是完美地被关联的，外推算法用于估计目标的位置
细	“具有外推的不完美地关联”模型	对观察报告采取了阈值方法的简单的关联衡量和属性匹配，外推算法用于估计目标位置
很细	“具有卡尔曼滤波的不完美地关联”模型	与上面模型一样的关联模拟方法，只是对于目标的位置估计采用卡尔曼滤波

此外，联邦中所需的管理和运行控制成员，剧情产生成员和数据采集成员也都要作设计开发。有了所有联邦成员以后，就可以将它们通过局域网或广域网集成起来。当前的集成方法大都遵循HLA/RTI，即按照 HLA 的规范进行集成、控制和数据交换。

7 试验评估

试验开展前，首先要弄清楚本次试验的目标，相关的计划，确定的试验剧情，包括红蓝双方的战斗序列、剧情区的时间框架、试验中的成员与持续时间，数据的收集方法以及用于评估分析的度量等。

试验开始后，整个试验活动通常是按计划进行

的，为了获得良好的试验结果，试验管理和运行控制成员要不断地监视试验过程中的各相关试验设备的状态，正确地控制处理各种发生的情况，保障试验记录的数据正确，评估结果可信。

试验结束后，对试验中各种记录数据要进行汇总处理。应用综合系统性能度量指标及其指标求解模型求得各种度量指标的定量值。在这一求解工作中，先要进行一系列处理，主要解决三个方面的问题：一是那些记录数据可用于评估计算，即所谓选择问题；二是确定记录中的目标与实际目标之间的对应关系，即所谓指派问题；三是记录数据有缺损、时间上有不一致等问题时怎么做预先处理，即所谓重构问题。最后参试人员要形成试验评估报告。

参考文献

[1] R.Seymour, A.M.Grisogono etc, The Role of Synthetic Environment in C4ISR Modelling and Simulation, 5<sup>th</sup>ICCRTS, 2000.

[2] J.Dahman etc, Creating System Integration Simulation Environment:Common Design Principles, A Component-Based Reference FOM and a System-of-System Federation Development Process, The 2003 ESIW.

[3] Single Integrated Air Picture (SIAP) Metrics Implementation, SIAP SE TF Technical Report [ADA 397225], 2001.

[4] Single Integrated Air Picture (SIAP) Common Reference Scenarios (CRS), SIAP SE TF Technical Report, July, 2002.

[5] Colleen M.Gagnon and Willian K.Stevens, Use of Modeling and Simulation (M&S) in Support of Joint Command and Control Experimentation:Navel Simulation System (NSS) Support to Fleet Battle Experiments, The 1999 CCRTS.

[6] Willian K.Stevens etc, Representation of Command and Control (c2) and Information Operations (IO) in Military Simulations, The 1999 ISMACC.

[7] L.J.Zavarelli etc, Live Virtual Constructive Experiments For C<sup>2</sup> Evaluation, 11<sup>th</sup>ICCRTS, 2006.

作者联系方式

通信地址：C<sup>4</sup>ISR 技术国防科技重点实验室（28 所分实验室）  
邮政编码：210007  
联系电话：025-84288076



# 战术互联网节点编号规则与应用研究

甘志春 李健 宋贤群

**摘 要:** 本文结合集团军及数字化机步师的典型作战编成, 提出了一种分层次、可推导、易扩展的战术互联网节点编号规则, 并给出了应用举例。这对于灵活高效的战术网络管理及参数分发具有重要意义, 对其 IP 地址与用户号码等编码方法也有借鉴与参考价值。

**关键词:** 战术互联网; 网络管理; 节点编号

战术互联网是在高度机动作战环境下, 为作战部队各级指挥员、参谋、分队、士兵、以及所操纵的信息系统与武器平台, 提供纵向贯通、横向链接的无缝隙信息交换网络平台。其网络结构复杂、组织变化频繁, 要求网络规划、参数分发、网络监控灵活高效, 便于力量调整和网络重组。这就需要有一个不同于设备物理识别号的节点编号, 从逻辑上来分层表示不同的单位、枢纽、平台和设备。为此, 本文在原野战地域通信网 4 位节点编号基础上, 结合集团军及数字化机步师的典型作战编成, 提出了一种分层次、可推导、易扩展的战术互联网节点编号规则, 并给出了应用举例, 旨在为战术互联网灵活高效的网络管理及参数分发提供新思路。

## 1 基本概念

节点编号不同于设备识别号。设备识别号, 通常在设备出厂时设定, 由设备类型、生产厂家及序号等构成, 具有唯一性和不可更改性, 其主要用于固定标识某一具体设备, 相当于设备物理号。节点编号, 也可称作设备管理号, 是按网络组织关系定位各节点为何单位、何枢纽、何平台、何设备的广义节点逻辑编号, 主要用于灵活高效的网络规划、参数分发、网络监控、设备更替和网络重组, 也具有唯一性, 但要求其编号可随不同的作战编成而变化, 具备可推导性、直观性、层次性。实际应用时, 通常可先由通信部门负责各节点编号的生成, 再由通信部(分)队按节点编号与相应的设备(识别号)进行绑定。

## 2 编号规则

### 2.1 基本思路

1) 在应用规模上, 目前的节点编号至少应能覆盖一个军以下作战部队, 具体可以集团军及数字化机步师的典型作战编成为例。

2) 在编码层次上, 按照“先大类、后小类”的分层编码方法, 体现出各节点是何单位、何枢纽、何平台、何设备的层次关系。

3) 在编号选择上, 采用十进制数字表示, 以便于在参数注入器上输入。

4) 在逻辑推导上, 依据典型作战编成, 采用可推导编码方法, 便于计算机和人工自动生成。

5) 在实际应用上, 可采用等长码与缩略码两种编码方式。一般机器处理采用等长码, 而人工输入可采用缩略码。

6) 在可扩展性上, 规则中应有备用码, 以便于扩展。

### 2.2 编号结构

根据上述基本思路, 节点编号可由级别、编成、平台和设备四个区共 9 位十进制数字组成, 其结构如表 1 所示。

### 2.3 规则说明

#### (1) 级别区

用 1 位码表示节点是部队编成中的何级别, 其编码规定如表 2 所示。其中, 0~2 用于军以上单位编码时的拓展。

表 1 战术互联网节点编号结构表

	级别	编成				平台		设备	
	Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8	Y9
军直属 编成	3	01-09 军各指		0	0	平台类+序号		设备类+序号	
		10-49 军干线		0	0	平台类+序号		设备类+序号	
		50-99 军直属			同“团以下”				
师（旅）直 属 编成	4	X 师	01-09 师各指		0	平台类+序号		设备类+序号	
			10-49 师干线		0	平台类+序号		设备类+序号	
			50-99 师直属			同“营以下”			
团直属 编成	5	X 师	X 团	01-09 团各指		平台类+序号		设备类+序号	
				10-99 团直属		同“连以下”			
营以下	6	X 师	X 团	X 营	Y 连 Y 排		平台/班号	设备类+序号	
说明	X=1-9, Y=0-9								

表 2 级别编码表

级别编号	级别
0—2	军以上（留作扩充）
3	军指挥所及直属部（分）队
4	师指挥所及直属部（分）队
5	团指挥所及直属部（分）队
6	营以下

（2）编成区

表示该节点在作战中的编成序列，其中军、师（旅）、团级编成区为 4 位数，营以下编成区为 5 位数。以进攻作战为例，对该区的使用说明如下。

当对军各指挥所、干线节点和直属战斗队、群进行编码时，编码规定如表 3 所示。其中编成区第 1、2 位可查表 3 得到，各指和干线第 3、4 位为 0；军直属战斗队、群后 6 位编码同团以下。

当对师（旅）各指挥所、干线节点和直属战斗队、群进行编码时，编码规定同表 3 所示。其中编成区第 1 位为师在军编成内序列号，第 2、3 位可查表 3 得到，各指和干线第 4 位为 0；师直属战斗队、群后 5 位编码同营以下。

当对团各指挥所、干线节点和直属战斗队、群进行编码时，编码规定同表 3 所示。其中编成区第 1 位为师在军编成内序列号，第 2 位为团在师编成内序列号，团各指第 3、4 位可查表 3 得到，团直属战斗队、组后 4 位编码同连以下。

当对营以下进行编码时，编成区第 1~3 位通过营的编成序号得到（第 1 位为师在军编成内序列号，第 2 位为团在师编成内序列号，第 3 位为营在团编成内序列号），第 4、5 位通过查表 4，生成连、排编码。

表 3 指挥所、干线、直属单位编码对照表（以进攻作战为例）

	0	1	2	3	4	5	6	7	8	9
0	军、师、团	基指	前指	后指	预指	技指				
1		干线节点 01	干线节点 02	干线节点 03	干线节点 04	干线节点 05	干线节点 06	干线节点 07	干线节点 08	干线节点 09
2	干线节点 10	干线节点 11	干线节点 12	干线节点 13	干线节点 14	干线节点 15	干线节点 16	干线节点 17	干线节点 18	干线节点 19
3	干线节点 20	干线节点 21	干线节点 22	干线节点 23	干线节点 24	干线节点 25	干线节点 26	干线节点 27	干线节点 28	干线节点 29
4		升空中继 1	升空中继 2	升空中继 3	升空中继 4	升空中继 5				
5	穿插	机降	反空降	机动炮	反装甲	特种 1	特种 2	特种 3	特种 4	特种 5
6	侦察	电子对抗	通信预备	工兵	工兵预备	防化	防化预备			
7	后勤基本保障	后勤前方保障 1	后勤前方保障 2			装备基本保障	装备前方保障 1	装备前方保障 2		
8										
9										

表 4 营以下分队编码对照表（以机步营进攻战斗为例）

	0	1	2	3	4	5	6	7	8	9
0	营	营指			侦察 分队	反装甲 分队	防空 分队	工兵 分队		
1	1 连指	1 排	2 排	3 排	4 排					
2	2 连指	1 排	2 排	3 排	4 排					
3	3 连指	1 排	2 排	3 排	4 排					
4	4 连指	1 排	2 排	3 排	4 排					
5	炮兵连指	1 排	2 排	3 排	4 排					
6										
7										
8										
9										

(3) 平台区

表示各指挥所、干线节点、直属战斗队、群、组的平台构成。其中，军、师（旅）、团级平台区为 2 位数，前一位通常为承载平台类型，若以指挥所和干线节点为例其平台类型对照表如表 5 所示。

表 5 平台类型对照表

平台类号	平台类型
1	指挥车
2	干线节点车
3	用户节点车
4	无线电综合车
5	.....

（以用户和干线节点为例）

3 应用举例

根据上述编号规则，按照先大后小，从单位—枢纽—平台—设备的分层编码思想，以某一集团军及数字化机步师进攻作战为例，战术互联网节点编号规则应用举例如下。

3.1 基于单位的节点编号

某师（旅）节点编号的等长码及缩略码。以集团军 2 师、军炮兵旅（群）、军防空兵旅（群）为例，其 9 位等长码可分别为 420000000、480000000、490000000，缩位码可分别用 42、48、49 两位来表示。其中，第一位“4”意为师（旅）级，第二位“2”、“8”、“9”可分别意为集团军 2 师（若为梯队式编成，其可为一梯队师、二梯队师、合成预备师等）、军炮兵群、军防空兵

而营以下由于各编成单位的平台较少，其平台区可用 1 位数表示。

(4) 设备区

用 2 位数表示各平台的设备构成。以基本通信车为例其平台设备对照表可如表 6 所示。

表 6 设备类型对照表

设备类号	设备类型
1	野战交换机
2	互联网控制器
3	微波接力机
4	超短波电台
5	.....

（以基本通信车为例）

群。

某团节点编号的等长码及缩略码。以集团军 2 师 3 团、2 师炮团、2 师防空兵团为例，其 9 位等长码可分别为 523000000、528000000、529000000，缩位码可分别用 523、528、529 三位来表示。其中，第一位“5”意为团级，第二位“2”意为隶属于 2 师，第三位“2”、“8”、“9”可分别意为 2 师 3 团（若为梯队式编成，其可为一梯队团、二梯队团、合成预备团）、2 师炮兵群、军防空兵群。

某营节点编号的等长码及缩略码。以集团军 2 师 3 团 2 营为例，其 9 位等长码可分别为 623200000，缩位码可分别用 6232 四位来表示。其中，第一位“6”意为营级，第二、三位“23”意为隶属于 2 师 3 团，第四位“2”别意为 2 师 3 团 2 营。

军某直属群的等长码及缩略码。以集团军电子

对抗群为例,其 9 位等长码可分别为 361000000,缩位码可用 361 四位来表示。其中,第一位“3”意为军级,第二、三位“61”意为军电子对抗群。

### 3.2 基于枢纽的节点编号

某师(旅)指挥所节点编号的等长码及缩略码。以集团军 2 师基指为例,其 9 位等长码为 420100000,缩位码可用 4201 四位来表示。其中,第三、四位两位“01”意为基指。

某师(旅)干线节点编号的等长码及缩略码。以集团军 2 师干线节点 1 为例,其 9 位等长码为 421100000,缩位码可用 4211 四位来表示。其中第三、四位“11”意为干线节点 1。

某团指挥所节点编号的等长码及缩略码。以集团军 2 师 3 团基指为例,其 9 位等长码可为 523010000,缩位码可用 52301 五位来表示。其中,第四、五两位“01”表示基指。

某营指挥所节点编号的等长码及缩略码。以集团军 2 师 3 团 2 营指挥(观察)所为例,其 9 位等长码可为 623201000,缩位码可用 623201 六位来表示。第五、六两位“01”为营指挥所。

### 3.3 基于平台的节点编号

某师(旅)指挥所通信车节点编号的等长码及缩略码。以集团军 2 师基指用户节点车 1 为例,其 9 位等长码可为 420103100,缩位码可用 4201031 七位来表示。其中,第五位“0”为填充位,第六位“3”表示“用户节点车”,第七位“1”代表此类通信车在此枢纽中为第 1 辆。

参考文献(略)

作者联系方式

通信地址:湖北省武汉市解放公园路 45 号通信指挥学院战略研究所

邮政编码:430010

联系电话:027-85968236

营以下作战平台节点编号的等长码及缩略码。以集团军 2 师 3 团 2 营长指挥车及其 3 连 2 排第 4 辆步兵战车为例,其 9 位等长码可分别为 623201100,623232400,缩位码可用 6232011,6232324 七位来表示。第五、六两位“01”、“32”分别为营指挥所、3 连 2 排。其中,第七位“1”、“4”分别代表营长指挥车、第 4 辆步兵战车。

### 3.4 基于设备的节点编号

某师(旅)指挥所通信车的节点编号。以集团军 2 师基指用户节点车 1 接力机 2 为例,其 9 位等长码可为 420103132。其中,第八位“3”意为微波接力机,第九位“2”为该设备在此车的序号。

综合以上四类节点编号规则,每类的节点编号都是在上一类节点编号的基础上扩充形成的,体现了编码的层次性和可推导性。

## 4 结束语

战术互联网编号编址是战术互联网组织运用的前提与基础。本文提出的一种基于集团军战役编成的可推导、层次性强、扩展性好的战术互联网节点编号规则,为战术互联网灵活高效的网络管理与参数分发提供了有力的支撑,对提高战术互联网的作战效能有着重要意义。

下一步将借鉴上述思路,对战术互联网中的 IP 编址、用户编号等编码规则进行深入研究。

# 美军电子信息系统体系结构及其评估方法研究

陈桂生 张新强 彭慧军 李瑛

**摘 要:** 本文对美军军事电子信息系统体系结构框架的设计开发和联合测试与评估的基本理念、基本方法和相关流程进行了研究探讨,注重分析美军构建从体系结构设计开发到联合测试与评估之间完整链条的目的、作用和基本过程。美军强调信息系统体系结构是由不同功能领域的众多子系统构造成的系统之系统,为增强系统之间的互通性与互操作性,提升整体作战效能,必须将体系结构产品聚集到作战环境中进行综合分析,通过联合试验与评估,提出改进或修改建议,最后由当局做出决议,实现系统的改进或升级,以更好地满足作战需求。这对于我军当前乃至今后军事电子信息系统体系结构的顶层设计,具有一定的借鉴意义。

**关键词:** 美军电子信息系统; 体系结构; 联合评估; JMACA

美国国防部一直在开展电子信息系统体系结构相关的工作,并取得了多项成果,如信息管理技术体系框架(TAFIM)、C4ISR 体系结构框架、联合技术体系结构(JTA)、国防信息基础设施公共操作环境(DII COE)、技术参考模型(TRM),以及当前研究的新进展——DoD 体系结构框架(DoDAF)和全球信息栅格(GIG)等,同时,美军认为,体系结构设计必须在联合作战和集成各军种能力方面加强努力,强调“部队最重要的转型不仅仅是武器系统,而是互联,以及充分增强能力”,在网络中心战中,信息优势的作用越来越重要,越来越依赖强大和复杂的 C4ISR 可互操作的体系结构,而在部署每个 C4ISR 体系结构之前,对其进行快速评估和改进将是提高作战人员信息优势的重要举措。本文对美军电子信息系统体系结构及其能力评估方法进行分析研究,期望对我军未来军事电子信息系统的体系结构研究提供有益的参考。

## 1 美军电子信息系统体系结构的进展

根据 IEEE 610.12 的定义,体系结构(architecture)是指一个被定义领域的组成单元的结构、它们的相互关系,以及指导它们设计和随时间演进的原则和指南。随着技术的发展和实践的深入,美军越来越认识到体系结构的重要性。美国国防部(DoD)一直在开展信息系统体系结构相关的工作,并且取得了多项成果。DoD 所提出、制定的一系列框架、指南和体系结构是构建 DoD 信息

系统的基础。

### 1.1 体系结构相关研究成果

从 20 世纪 90 年代初到 20 世纪末将近 10 年的时间中,DoD 先后开展了多项体系结构相关的研究,其成果大致可以概括为以下几个方面。

#### 1.1.1 信息管理技术体系结构框架

信息管理技术体系结构框架(TAFIM)是最早为开发支持 DoD 使命的信息系统而制定的策略和指南,它为开发满足特定作战和功能需求的技术体系结构提供服务、标准、设计概念、组件及配置指导。1993 年 TAFIM 成为促进 DoD 信息系统集成的唯一框架,1997 年 1 月宣布了 TAFIM 的第 3 个版本,由于形势的发展在 2000 年 1 月 TAFIM 被宣布取消。TAFIM 在 DoD 信息系统体系结构的研究发展过程中,发挥了重要的作用。其中,TAFIM 3.0 由 8 卷组成,包括技术参考模型(TRM)、体系结构概念和设计指南、基于标准的体系结构规划指南、开放系统项目负责人指南、DoD 目标安全体系结构(DGSA)、采用的信息技术标准(AITS)以及 DoD 人机界面样式指南。

#### 1.1.2 C4ISR 体系结构框架

为了加强从上到下的统揽指导作用和从下向上的设计灵活性,基于体系结构产品的框架研究是关于体系结构开发与评估的统一指南。美军 C4ISR 体系结构框架的宗旨是为各总司令部、各军种和国

防部各厅局提供一个通用的、统一的体系结构开发方法,以便使用此方法开发他们各自的各种体系结构,并保证所开发的各体系结构之间是互相关联的,在联合和合成机构之间是可比较和可集成的。虽然 C4ISR 体系结构框架特别瞄准 C4ISR 系统,不过该框架内确定的方法很容易扩展到国防部的人员管理、系统采购和财务等其他领域,美军 C4ISR 体系结构框架被宣布成为 DoD 体系结构框架发展的战略方向。

### 1.1.3 联合技术体系结构

标准和指南是结构框架的主要载体,联合技术体系结构(JTA)规定了一套通用的强制性信息技术标准及指南,用于战术、战略及支持基础系统。JTA 定义的服务领域、接口和标准适用于所有的 DoD 系统,为 DoD 系统的无缝互操作提供基础。JTA 的核心包括信息处理标准,信息传送标准,信息建模、元数据和信息交换标准,人机接口标准以及信息安全标准五大类标准。

### 1.1.4 国防信息基础设施公共操作环境

为适应开放系统的开发和集成,尤其是开放互联环境下的系统互操作性,国防信息基础设施公共操作环境(DII COE)提供了标准的环境及一套成品(OST)组件标准以及一套编程规范。DII COE 被看作是构建互操作系统的方法,是包含可重用软件组件集合的参考实现,是支持使命应用的软件基础结构。在 COE 中包括核心 COE、基础服务、公共支撑应用、开发工具和共享数据工程(SHADE)。目前,美军的全球指挥控制系统(GCCS)、全球作战支持系统(GCSS)等都是建立在 COE 之上的。DII COE 中一些与 JTA 不一致的标准将被取消,并且在 DII COE 演进过程中必须保持与未来 JTA 中标准的一致性。

### 1.1.5 技术参考模型

结构框架不仅需要宏观的概念性框架,更细粒度的技术性框架也是至关重要的。美军的技术参考模型(TRM)作为 DoD 公共的概念性框架,确定了公共的词汇表,描述和定义了支持 DoD 信息系统技术体系结构设计和互操作框架开发的服务、接口以及它们之间的关系,是信息系统选用标准和结构化的更细粒度的基础。TRM 最初是作为 TAFIM 中的一卷出现的,在 TAFIM 取消后 TRM 继续发

展,独立的 TRM1.0 于 2000 年正式颁布,2001 年 4 月又提出了 TRM 2.0。TRM 是 JTA、C4ISR 体系结构框架及 COE 的共同基础。TRM 包括应用软件、应用平台和外部环境三种实体以及应用程序接口、外部环境接口两种接口,在 TRM 的详细模型中,又进行了进一步的划分,标识出了服务领域和它们的接口。

## 1.2 体系结构框架的进展

### 1.2.1 DoD 体系结构框架(DoD Architecture Framework)

随着情景敏感开发和基于场景的需求描述设计技术日臻成熟,美军 DoD 体系结构框架更注重对全球不同应用场景的针对性,与 C4ISR 体系结构框架相比,其最主要的改进包括基于设想的用途确定体系结构内容的指南;注重使用体系结构支持 DoD 的需求生成系统(RGS),规划、计划和预算系统(PPBS)和后勤管理系统;以及更加强调体系结构的数据方面。DoD 体系结构框架主要反映了美军在开发和应用体系结构描述方面已经获得经验。

### 1.2.2 全球信息栅格(GIG)

随着“规模化定制”成为网络时代软件、硬件乃至大型系统设计研发的主要方式,电子信息系统更加强调对基于能力的适应性的满足。从体系结构的角度看,美军 GIG 是一种 C4ISR 系统的新体系结构,其能力的核心是建立能够“定制 C4ISR 能力”的信息环境。GIG 体系结构遵循了 C4ISR 体系结构框架的三种视图。当前版本的 GIG 体系结构在开发时,特定想定的作战视图和系统视图是通过集成现有的体系结构产品而构建的,技术视图则基于 JTA。GIG 作为下一代的国防信息基础设施,被看做是 DII COE 的扩展,目前 DII COE 也被称之为 GIG COE。对于技术参考模型,在 2002 年 3 月颁布的 TRM 2.0 中,指出 TRM 2.0 定义和描述了用于支持集成体系结构、JTA、C4ISR 体系结构框架及 COE 开发的 GIG 服务、接口和它们之间的关系。

### 1.2.3 体系结构框架产品定制的基本方法

C4ISR 框架中定义的三种体系结构包括作战视图、系统视图和技术视图,这三种视图之间是紧

密的相互制约和相互连接的关系,在逻辑上结合在一起完整地描述系统的体系结构。**C4ISR** 体系结构框架中对体系结构产品的定制方法,大致分为五个环节,各个环节相互关联,反复迭代,在功能上和逻辑上承上启下,各个节点相互支撑,相互制约,最后形成一个不可分割的整体。而各环节、各模块在功能上、逻辑上的一致性、完整性以及相互之间的嵌入和支撑关系,尤其是互联互通互操作性等,为后续的联合测试与评估提供了良好的目标和接口。

1) 基于特定应用场景确定预想用途。在许多情况下,没有足够的时间、资金或资源从上到下建立一个无所不包的体系结构。体系结构应当根据一个特定的目的来建立,可以是业务过程的重新设计、系统采购,系统体系的升级或集成、用户培训、互操作的评估或任何其他目的。在开始描述体系结构前,一个机构必须尽可能明确一些问题,如试图用体系结构研究什么问题,期望体系结构帮助回答什么问题,以及读者和用户的兴趣和观点。此外,还必须考虑期望完成的分析类型。这样集中瞄准一个问题,将提高体系结构的开发效率,并使最终形成的体系结构更为合理和有用。

2) 基于预想任务使命定义体系结构的系统边界域。主要涵盖应用范围、背景、环境和任何其他需要考虑的假定。一旦确定了目的和用途,体系结构的预期的边界域也就可以确定。要考虑的问题包括体系结构的范围(行动、功能、组织机构、时间等)、合适的详细程度、在“一个较大的概念”中体系结构工作的背景、作战想定、应考虑的姿态和地理范围、预计的经济状况以及在所设想的时间内特定技术的可用性和能力,而且不仅限于这些问题。有些计划管理因素也会对上述问题产生影响。

3) 基于问题域边界提取特定体系结构的特征集。为达到体系结构的目的,首先要提取和分类描述体系结构的特征集合。特征集应尽可能完备、较少冗余和可裁剪、可扩展。如果必要的特征被遗漏,体系结构的效能将极大地降低。而如果包含了不必要的冗余特征,体系结构将会被不必要的细节干扰。应当特别注意考虑体系结构的未来用途,这样在资源有限的情况下,体系结构能够适应今后的剪裁、扩展以及复用。

4) 基于特征集定制体系结构视图和主要支撑产品。体系结构视图和支撑产品是体系结构的基本

物化形态,是承载总体意图的基本载体。首先开发定制对所有体系结构必须的基本产品,包括那些描绘必需特征的支撑产品。在此基础上进一步构建一套完整的体系结构视图和支撑产品,它们由基本产品、所需的支撑产品和由体系结构特定需求驱动的单一定义的产品组成。为有利于同其他体系结构的集成,关键是要包括与适用的联合的和多国组件的关系的全部描述。如果需要,体系结构应当尽可能有效地进行剪裁。为此,在开发过程中的不同阶段,对体系结构进行一些原理性的试验分析是很有用的。

5) 基于设想的场景分析评估和检验体系结构产品。根据设想的特定目的建立体系结构,必须强调指出,体系结构促进并使得设想的最终目的成为可能,但体系结构本身并不提供结论或答案。因此,必须进行人工分析和可能的自动分析。**C4ISR** 体系结构框架旨在促进开发足够完善的、可以理解的和可集成的体系结构,以便成为分析的基础。

## 2 美军电子信息系统体系结构的联合评估

美军在开发体系结构框架的进程中深刻地认识到,随着信息优势在军事作战尤其是网络中心战中的作用越来越明显,对 **C4ISR** 体系结构进行联合评估也相应地日益重要,美军于 2001 年 10 月开始了联合试验和评估计划(JTE)下的名为“评估 **C4ISR** 体系结构联合方法(JMACA: *Joint Methodology to Assess C4ISR Architectures*)”的研究,展开对 **C4ISR** 体系结构进行联合测试和评估,并探索对体系结构诸要素及其相互关联、相互依存和相互制约的必要性、可行性以及整体性能进行综合评价的方法、途径和关键技术。

### 2.1 体系结构评估的定位和作用

美军对 JMACA 的定位,就是通过将现有的分析工具和数据库结合起来快速评估联合 **C4ISR** 体系结构的能力,使得 JMACA 过程能够从各军兵种挑选相适应的作战部队,搜集众多系统的信息,指定参与联合试验部队或演习的部队,分析体系结构在作战环境下的性能,达到深入地了解体系结构之目的。其所起到的作用可以概括为以下四个方面。

1) 为 C4ISR 的综合集成奠定基础。JMACA 提供了对作战体系结构进行评估的能力, 改善了作战需求的集成, 提高 C4ISR 需求评估能力, 以达成支持联合作战的目的。

2) 为 C4ISR 互操作性提供风险论证。JMACA 致力于用分析工具和数据库对系统风险进行量化分析, 使得风险论证有了衡量的标准, 从而能对执行联合任务过程中功能上的线程风险进行量化分析。

3) 进行快速作战分析。JMACA 使得通过数据挖掘过程读取各自分散的联合数据资源成为可能, 从而提高了对 C4ISR 体系结构评估的速度和准确率。

4) 与联合团体合作, 加快 C4ISR 集成和转型计划。JMACA 从开始计划研究起, 就与各个团体紧密合作, 参与国防部及各军兵种的主要计划中, 充分发挥评估效能, 致力于使空中、水面、陆地、水下 C4ISR 作战和系统体系结构可以互操作, 最终达到加快众多 C4ISR 体系结构的集成和转型的目的。如, 与国防部合作全球信息网格计划; 与海军/海军陆战队合作力量网计划; 与空军合作 C2 星座计划; 与陆军合作目标部队计划; 与海岸警卫队合作集成深水系统计划等等。

## 2.2 体系结构评估的过程和方法

美军开展对 C4ISR 体系结构进行联合测试和评估, 其基本过程包括明确工具和分析需用的数据、明确体系结构范围的风险、有选择地对高风险区域进行分析、提出体系结构的建议。体系结构评估涉及的关键技术包括以下五个方面的方法。

1) 通过数据挖掘, 收集系统配置和风险信息。数据挖掘是从大量的、不完全的、有噪声的、模糊的、随机的数据中提取潜在的、不为人知的有用信息、模式和趋势。通过数据挖掘, 有价值的知识、规则或高层次的信息就能从数据库的相关数据集合中抽取出来, 为决策提供依据, 从而使数据库作为一个丰富可靠的资源, 为知识归纳服务。

2) 通过风险评估, 对体系结构各种视图进行广泛的分析和综合。风险评估是指依据有关信息安全技术与管理标准, 对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估系统面临的威胁以及威胁利用脆弱性导致安全事件的可能性。评估安全

事件一旦发生可能造成的危害程度, 提出有针对性的抵御威胁的防护对策和改进措施。由于系统设计缺陷、隐含于软硬件设备的缺陷、系统集成时带来的缺陷, 以及可能存在的某些管理薄弱环节, 尤其当网络与信息系统中拥有极为重要的信息资产时, 都将使得面临复杂环境的网络与信息系统的潜在着若干不同程度的安全风险。

3) 通过多粒度分析, 评估体系结构不同粒度层次上的功能和目标任务。对系统进行风险评估后, 确定了优先的系统需求, 对整个体系结构中涉及高风险和关键任务的诸要素, 需要对其进行进一步的更小粒度的分析评估, 尤其是系统之间如何互连互通, 以及在互连互通中会出现怎样的问题, 及其给作战带来怎样的风险等。多粒度分析就是要针对不同优先级设置相应的指标体系、对体系结构中诸要素分解为相应的各种状态, 实现自上而下的定性概念分解与自下而上的定量分析集成相结合, 完成对不同粒度需求的功能和目标任务的测试和评估。

4) 采用端到端测试试验方法, 对物理的硬件和相应软件进行测试。端到端测试运用高级分布式仿真建立增强环境来测试 C4ISR 系统, 它是为评估高级分布式仿真的效用以支持 C4ISR 系统测试而设计的。目的是为传感器到武器系统提供一个完整的、坚固的界面设备, 包括额外的中间节点, 这些中间节点将建立在战术环境中。测试使用高级分布式仿真在军级追踪完整的战场步骤线程, 从目标侦察到目标分配和交战。

5) 紧密结合作战使命进行作战目标和任务分析。美军通过成立专门的作战分析小组, 紧密结合作战使命对作战目标和任务进行分析。小组成员将上述几个环节获取的数据, 包括风险评估、粒度分析、端到端测试等得出的结果和数据, 聚集到作战环境中进行综合分析, 然后向包括联合特遣部队和联合部队司令官在内的决策当局提出改进或修改建议, 最后由当局作出决议, 实现系统的改进或升级, 以更好地满足作战需求

通过上述联合测试与评估, 将得到的结果向权威机构联合特别工作组和联合部队司令官提出建议要改进的地方, 最后加以实施。美军通过从体系结构设计开发, 到联合测试评估, 形成关于体系结构产品的完整链条。



### 3 结论：从设计开发到联合评估的闭环控制

纵观美军电子信息系统体系结构产品的设计开发，剖析其体系结构联合测试与评估的基本流程，不难发现美军正在逐步形成电子信息系统从体系结构设计开发到联合评估的总体闭环控制。联合作战和网络化扁平指挥需要一体化的信息系统。而一体

化信息系统体系结构是由不同功能领域的众多子系统构造的系统之系统，为增强系统之间的互通性与互操作性，提升整体作战效能，必须将体系结构产品聚集到作战环境中进行综合分析，通过联合试验与评估，提出改进或修改建议，最后由当局做出决议，实现系统的改进或升级，以更好地满足作战需求。这对于我军当前乃至今后军事电子信息系统体系结构的顶层设计，具有重要的借鉴意义。

#### 参考文献

- [1] Joint Methodology to Assess C4ISR Architectures (Sep 2002), [http:// www.jmaca.jte. osed.mil/index.html](http://www.jmaca.jte.osed.mil/index.html)
- [2] 李德毅等. 发展中的指挥自动化. 北京: 解放军出版社, 2004.
- [3] 中国国防科技信息中心译. 网络中心战—美国国防部呈交国会的报告, 2002
- [4] 彭慧军等, 基于 PD—效用函数的风险决策方法, 信息工程大学学报, 2004.3

#### 作者联系方式

通信地址: 北京市丰台区大成路 13 号 Z00

邮政编码: 100039

联系电话: 010-66820126

# 系统集成：谋求信息时代战斗力的跃升

陈鹏 孙晋华 曹伟东 张海陆

**摘要：**信息作战条件下，作战已经成为一种体系与体系、系统与系统的对抗，系统集成作为信息作战的“粘合剂”是提高我军战斗力的最根本的方法和途径。本文从战斗力的生成模式出发，讨论了基于信息作战体系形成、构建、运行机理下系统集成对提升我军战斗力的重要作用。

**关键词：**系统集成；信息作战；战斗力

提升战斗力，是军队建设首要和核心的任务。面对由机械化作战向信息作战转变的关键时期，信息作战已经成为一种体系与体系、系统与系统的对抗，我们一定要转变战斗力生成模式，树立作战体系综合集成的观念，以形成信息作战能力为目标，扎扎实实推进战斗力的全面提升。

## 1 信息作战条件下战斗力生成模式的转变

### 1.1 突破“要素分离”型军事思维

传统军事思维认为，物质和能量是构成军队战斗力的主要方面。追求更大的杀伤力、更快的机动性、更强的防护力，是贯穿于历次军事变革活动的一个基本思路，其实质是在解决和处理问题时只看重个体因素，忽视整体全貌。表现在战斗力生成模式上，主要是陆、海、空等各军兵种单独发展，自成体系，横向联系少；武器装备的发展采用“烟囱式”，只注重研制一代比一代先进的武器系统，不注重武器装备之间的横向互通互动；在军事组织体制中，只强调某个或某些单位的重要，不注重以结构谋功能，导致不能从整体上看个体，难以谋求整体效能的提升；在战争指导上，主要表现为以线式的行动理念，追求双方作战系统内各构成要素的对抗，以量的变化来削弱对方的整体实力，注重各个击破，积小胜为大胜等。这种“要素分离”型的军事思维在一定历史时期具有其合理性，但随着信息化战争的来临，战争日益成为体系与体系的对抗，它已不能适应一体化联合作战的需要，难以有效地促进战斗力的提升。因而，在发展思路，要使过去的“要素分离”型向“体系融合”型转变，在

1+1>2 的追求中，谋取战斗力的整体性跃升。

### 1.2 建立“体系融合”型军事思维

体系化军事思维是信息时代的产物，是建设信息化军队，打赢信息化战争的主导思维方式。其本质是用“系统论”的观念来处理军事问题，开展建设活动。按照系统论，作战体系是由许多相互作用的子系统组成的复杂自适应系统。在子系统的相互作用下，复杂自适应系统“涌现出子系统所不具有的整体行为”。即通常所说的“结构决定功能”，“1+1>2”。体现在作战体系上，就是构成体系的各单元、要素对体系整体效能的贡献不是他们各自能力的线性加和，而是具有放大或缩小功能的非线性作用（结构合理，系统的整体功能大于各子系统的线性叠加之和，结构不合理，系统的整体功能小于各子系统的线性叠加之和）。

总之，信息化武器装备的大量运用，使战场空间一体化、力量结构一体化、作战行动一体化。在此情况下，战斗力的生成模式就思维和理念而言，必须实现由要素型向体系型的转变，着力于系统结构的整体性和稳定性，促进信息作战条件下战斗力的形成和跃升。

## 2 基于信息作战体系形成机理的信息系统系统集成是形成战斗力的基础

### 2.1 信息作战体系的形成机理

信息作战较之机械化作战，最根本的区别是作战的主导能量由人的体能、化学能、机械能等转变为信息能，其作战效果突出地表现为信息能主导下的作战力量使用、作用目标选择和作战效果实现的

精确性。

信息作战通过信息能对机械能的主导、整合作用,提高了作战力量的整体机动速度,可以精确安排各作战力量以最科学的方式实施机动;也提高了作战力量的整体防护能力,通过对战场态势的全面了解,从而可以有的放矢地主动采取规避、防护措施;还提高了作战力量的整体打击效果,信息与武器装备的有机结合,使打击的针对性更强,效果更为精确。信息能使战场作战力量形成一个更高效和更具有战斗力的整体。

其次,由于信息作战战场信息网络的普遍链接和战场态势的实时共享,给各级指挥人员创造了一个不受地理空间距离概念和地形特征限制的协作空间,它们可以分布在战场任何需要的地点,通过信息网络在空间内进行资源的共享、信息的交流和指令的下达,完成所有的指挥控制工作。因此,在信息作战中,由信息网络将信息探测能力、指挥控制能力和火力打击能力融为一体,实现感知——决策——行动——评估过程的一体化,无论何时、何地,都可以对各种类型的目标做到实时发现、实时打击,实现近实时的反应。这就形成了信息时代的信息作战体系。

## 2.2 信息系统综合集成是形成战斗力的基础

基于上述机理,在信息作战条件下,能否有效形成战斗力已不再取决于战斗部本身所处的系统,而是取决于更大、更广泛的信息系统对其的正确引导和支持。因此,作战体系必然谋求最大获取、最佳处理、最快传递信息的信息流动程序,要求信息流动必须符合信息固有的时效性、共享性、可处理性的特性。信息作战体系信息流程的主导形式,是减少信息流动“递阶”层次,在纵向流动的基础上,更注重信息横向流动的信息流程网络一体化,以确保信息有序、合理、快速流动,实现信息流动“横向一体、纵向贯通”的目标。

因此,只有实现信息系统的综合集成,才能有效利用信息技术,将武器平台、作战体系进行整合,通过内部渗透、外部融合等方法,实现所有信息系统的互联互通,这是形成战斗力的基础,也是最关键的部分。信息系统既是火力打击、情报侦察、指挥控制、综合保障等作战要素一体化的“粘合剂”,也是军队整体作战能力提高的“倍增器”,同时又是军队信息化建设的核心工程,其质量直接

影响作战体系的一体化水平,其建设速度直接影响着军队信息化建设的进程。只有搞好了信息系统层次上的综合集成,才能为作战要素、武器平台、作战体系的综合集成奠定良好的基础,才能实现不同作战系统之间的高度融合与无缝链接,从而达到互联互通,整体调控。

## 3 基于信息作战体系构建机理的作战要素综合集成是形成战斗力的核心

### 3.1 信息作战体系构建机理

信息作战,其作战体系的构建机理,主要体现在体系内诸单元、要素的组织结构及相互间的关系上。体系构建的基本方式是以信息为纽带,以网络为基础,对各单元、要素进行综合集成。

在信息作战条件下,作战战场空间原有的单一纵向发展模式已为网络化、信息反馈化的一体化多维战场所取代,作战效果已取决于战场上单个作战物质手段的效能和诸多种作战物质手段效能的综合。信息关联使作战体系构成的各部分联接得更为协调和紧密,使战场上的人、武器、作战单元等一切战斗力要素具有了一种基于信息的网状运动的高级系统的关系,因而作战体系各单元、要素之间具有了新的结构,也就产生了新的整体性,使得作战体系的效能大小,由机械化作战中构成体系的各单元、要素的线性加向联接各要素的信息结构力(由信息为联接纽带而形成的结构力)倾斜,并使其成为作战体系效能形成的重心。

因此,构建信息作战体系的基本方式就是作战要素的综合集成。即充分利用信息技术,从横向上对各种武器装备进行“一体化”改造,使其在具有更好的通用性、交互性和联动性的基础上,根据战场环境和特定的功能需求,来安排和处置作战单元与作战单元之间、作战装备与作战装备之间、作战装备与武器系统之间、传感器与作战装备之间、传感器与火器之间的联结和组合,以及它们在战场空间的分布情况。

### 3.2 作战要素综合集成是形成战斗力的核心

基于上述机理,按照一体化作战的要求,将各个作战单元内的情报侦察、指挥控制、火力打击、综合保障等不同作战要素进行合理配置,有机融

合,形成整体,这是形成一体化作战能力的关键。它不但为信息系统综合集成提出具体作战需求,又为作战体系综合集成提供基本要素,在整个作战体系的综合集成中,起着承上启下的作用。因此,信息作战条件下形成战斗力必须以作战要素综合集成为核心。

作战要素的综合集成,目的是通过科学配置和优化组合,建立起作战系统、体系内部的有序结构,使其能够充分发挥各个作战要素的效能,达到“整体大于部分相加之和”的效果。其基本着眼点,一是着眼作战需求,消除各作战单元指挥和管理机构中职责不清、功能重复、相互掣肘等不合理现象;二是对装备、情报、指挥及后勤保障系统进行一体化构建,对作战单元自身内部结构和外部相关支援、保障系统进行一体化整合,从而实现组织结构最优、作战系统一体、整体功能跃升;三是信息作战体系必须具备较强的防止体系的单元要素被彻底损毁、信息流被阻塞中断的能力。为此,组成系统的单元、要素在功能上要具有一定的重叠区,可以相互进行一定程度的弥补,在数量上要具有一定的备份,使体系结构具有一定的替代、补偿功能。

## 4 基于信息作战体系运行机理的作战体系综合集成是形成战斗力的目标

### 4.1 信息作战体系运行机理

信息作战,以信息感知和利用为主线,通过系统集成方法,将各军兵种的作战平台、武器系统、情报侦察和指挥控制系统以及后勤保障系统等作战单元、要素,整合为一体化、智能化的大系统,战场对抗表现为体系与体系的整体对抗、综合对抗。

信息作战体系的整体效能不仅取决于各单元、要素的自身效能,更取决于系统的整体结构。因此,信息作战的基本战法是通过破坏敌作战体系局部结构的破坏,降低其结构力的形成,抑制其整体效

能的发挥,进而对其具体目标进行物理摧毁、消除,剥夺其抵抗能力,直至其屈服。具体讲,就是通过分析敌体系结构、关节及其相互之间的本质联系,找准敌作战体系中整体和局部的支撑体系联动的数据链等起关键作用的目标。灵活运用信息攻击、火力打击、兵力突击等多种手段,实施突然、猛烈的破击。同时,抓住敌作战体系被割裂,局部陷于孤立,作战体系效能的生成与聚合受到破坏,具体作战单元、要素难以从体系获得有力支援的时机,以多种力量、多种方式对构成其作战体系的具体目标进行彻底的实体摧毁,清除恢复其体系和效能的物质基础。因此该种战法既不是仅仅、完全依靠体系破击,也不是像机械化作战中通过对敌作战单元、要素摧毁破坏的累积来战胜对方,而是二者的有机结合。体系破击是对具体目标进行实体摧毁的基础和条件:对具体目标的实体摧毁是体系破击行动的延伸和效果的保持。

### 4.2 作战体系的综合集成是形成战斗力的目标

基于上述机理,信息作战体系的对抗是整体对抗、综合对抗,只有通过作战体系的综合集成,在信息网络综合集成的支撑下,以作战要素的综合集成为基础,实现各军种作战体系的综合集成和一体化,才能真正具备遂行三军一体化联合作战的能力。这是形成战斗力的最终目标,也是综合集成的高级阶段。实现了作战体系的综合集成,也就实现了信息作战的综合集成,它是军队信息化建设和实现战斗力跃升的最终目标。

作战体系的综合集成,必须针对当前存在的迫切需要解决的现实问题,理顺各军种相对分立的指挥体制和指挥关系,转变“烟囱”体制,简化指挥层次,打破部门壁垒,实行纵向衔接、横向一体、无缝互联的体系结构。这样不仅能够为信息网络和作战要素的综合集成创造更好的条件,而且能加快作战体系综合集成的进程。

参考文献(略)

作者联系方式

通信地址:合肥市黄山路460号电子工程学院401教研室

邮政编码:230037

联系电话:0551-5767673 13721032738

# 军事信息资源共享服务体系构建研究

戴剑伟 吴照林

**摘 要:** 随着我军信息化建设的不断推进, 军事信息资源的管理与利用问题日益突出。论文分析了军事信息资源管理与利用中存在的问题, 阐述了军事信息资源共享服务体系构建的内容和主要功能, 提出了基于 SOA 的军事信息资源共享服务体系的技术构架。

**关键词:** 军事信息资源; 共享环境; SOA

## 1 引言

随着我军信息化建设的不断推进, 日常办公、军事训练、作战演习、军事科研、作战决策等对军事信息资源的需求量不断增大, 军事信息资源的管理与利用问题日益突出。由于现有的军事信息系统是按军兵种和各业务部门职能分工组织建设, 虽然强调统筹规划、统一标准, 但由于缺乏标准一致性检验和认证, 加之各单位建设基础不同、使用需求不同、建设重点不同等原因, 造成信息资源分割严重, 信息孤岛大量存在, 资源获取与可用性差, 信息交换共享十分困难。存在以下几个主要问题。

(1) 数据描述局部有序, 整体规范欠缺, 严重影响资源使用与共享

在全军各种信息系统建设中, 多从自身业务出发来构建信息系统, 业务数据固化于软件实现中, 且信息资源单独管理, 造成了业务与数据的相对自我封闭。对需要跨部门共享的业务信息, 因其描述格式、描述方式均不统一, 标准化程度低, 导致大量事实性信息孤岛出现, 且不同孤岛间的数据获得与使用困难。如何建立军事信息资源标准化数据体系, 保证数据表达、处理、展现的规范化已经成为当前军队信息化建设亟待解决的重要问题。

(2) 资源共享模式单一、可扩展性不强, 信息组织与发现步履艰难

基于传统技术构建形成的各种应用, 因技术手段制约, 共享实现常以点对点的信息共享和交换方式为主, 这种模式存在方法欠灵活、系统瓶颈明显、可扩展性弱, 并且部署与实施复杂程度高, 不利于各取所要求下的业务开展需要。如何构建灵活、易扩展的资源共享模式, 以保证合法用户能够及时发现所需的共享信息资源, 需要有效的信息组

织方式作为支撑。但是客观上由于这些信息来源于不同地域、不同部门, 必然导致数据处理的不一致性问题, 所以, 有关信息的组织与发现成为资源利用与共享中的又一个难点。

(3) 应用系统多自成体系, 信息资源获得与使用机制僵硬

现有各种信息系统中, 用户通过凝集在业务软件实现中的信息资源视图方式来实现对业务功能的满足, 由于受不同部门职能分割影响, 重复管理、重复维护, 不仅使工作量大大增加, 而且极易产生数据的不一致现象; 现有信息资源的重复设置、强行割裂、应用系统扩展能力不强等弊端已经成为影响军事信息资源获取与使用的关键问题之一。

这些问题的症结是缺乏统一规划、规范建设的军事信息资源管共享服务体系。军事信息资源共享服务体系是应用现代信息技术, 整合离散的军事信息资源, 构建面向全军的网络化、智能化的管理与共享服务体系, 实现对军事信息资源的规范化管理及其高效利用, 最大限度地发挥军事信息资源的潜在价值, 从而为我军日常办公、军事训练、作战演习、军事科研、作战决策等提供强有力的信息资源支撑, 实现我军信息化建设跨越式发展。

## 2 共享服务体系构建的内容

军事信息资源管共享服务体系构建的内容包括标准规范和管理制度、数据资源建设、网络及软硬件基础平台、安全系统建设。

### 2.1 标准规范和管理制度建设

标准规范和管理制度是军事信息资源共享体系

成功建设、规范化运行和发挥军事信息资源效益的有力支撑和可靠保障。因此,军事信息共享服务体系建设的首要任务应围绕信息采集、组织、分类、保存、发布与使用等信息生命周期各环节,对我军已有的标准规范和管理制度进行梳理、修改、完善、补充。针对军事信息资源建设现状,为更好继承发展,应建立适应军事信息资源共享需求的通用标准和专用标准。

### 2.1.1 通用标准

通用标准是军事信息资源共享服务中的共性的相关标准,包括三类标准:数据类标准、服务类标准、管理和建设类标准。

数据类标准包括元数据标准、分类和编码、数据内容标准等。元数据标准用于规范元数据采集、建库、共享和应用。分类和编码作为信息资源分类和编码时共同遵守的标准。数据内容标准用于数据的规范化改造、共享及应用。

服务类标准是提供军事信息资源共享服务相关标准,包括数据发现服务、数据访问服务、数据表示服务和数据操作服务。涉及军事信息资源的发布、表达、交换、共享等环节,规范军事信息资源数据的转换格式和方法互操作的方法和规则,以及认证、目录服务、服务接口等方面。

管理和建设类标准用于指导系统建设、规范系统的运行。包括质量管理规范、数据发布管理规则、运行管理规定、信息安全管理规定等。

### 2.1.2 专用标准

专用标准就是根据通用标准制订出来的,满足各军兵种信息资源共享需求的标准,重点反映各军兵种数据特点的数据类标准。比如军事通信与指控元数据内容标准、军事通信与指控数据分类与编码标准等。

## 2.2 数据资源建设

数据资源是军事信息资源共享服务的基础。数据资源建设包括:元数据库建立、管理与维护,主体数据库建设和数据的存储与运行维护。

### 2.2.1 元数据库建立、管理与维护

遵循元数据有关标准,采用统一标准的元数据工具进行元数据库的建立、管理与维护。元数据工

具应具备的主要功能包括:元数据建立、删除、备份、恢复、更新、一致性验证、内容正确性验证、导入、导出,以及元数据库的访问控制、用户管理等。

### 2.2.2 主体数据库建设

主体数据库是军事信息资源共享服务体系的基本单元,是提供系统、可靠的数据内容服务的基础。主体数据库主要是用来刻画和反映各军兵种领域内的基本数据状态,能满足各军兵种军事活动需要的数据集。比如通信兵的主体数据库有:通信装备数据库、通信资源数据库、无线频谱数据库等。它主要由各军兵种根据相关数据标准进行数据采集、加工和汇总,或者改造已有数据库而成。同时还建立起数据采集、加工、汇总、更新和使用的长效管理机制,使军事信息资源数据能够不断扩展、完善,保证数据的一致性、鲜活性和准确性。

### 2.2.3 数据的存储与运行维护

军事信息资源数据的存储策略采用基于网络的、以分布式数据存储为主、集中式数据存储为辅的数据存储模式。其中核心元数据和以及更新周期较长的数据库以集中式存储为主,其他各军兵种数据库可采用分布式存储。需要制定数据库备份策略和恢复计划,定期对数据库和日志文件进行备份,以便发生故障时利用备份数据将数据库恢复到备份式状态。根据用户需求、共享分级分类规定,给各级用户授予不同的访问权限;使用数据库管理系统监测系统性能参数工具监测数据库运行过程中的一切参数,并进行分析,调整和改进数据库性能。

## 2.3 网络及软硬件基础平台建设

网络及软硬件基础平台是军事信息资源共享服务体系发挥作用的物理基础,包括硬件平台和软件平台。硬件平台主要包括计算网络、专用服务器(包括应用、数据库、备份等服务器)、海量存储设备等。软件平台主要包括大型通用关系数据库管理系统、搜索引擎、电子邮件、FTP等软件系统。

## 2.4 安全系统建设

军事信息资源包含大量各种密级的数据,保证军事信息资源数据的安全在当前复杂的安全环境形势下尤为重要。因此按照军队有关安全标准规范和

条例,建立完善的安全技术框架,包括网络防火墙、入侵监测、病毒防护、身份认证、访问控制、授权管理等安全基础设施。

### 3 共享服务体系主要功能和技术构架

#### 3.1 主要功能

军事信息资源共享服务体系的主要功能包括:服务资源管理、目录服务、交换服务、信息服务、安全服务。

##### 3.1.1 服务资源管理

利用分布数据库技术、数据仓库技术、元数据技术和网络技术,建立以分布式为主、集中式为辅的标准化数据管理系统,开展数据采集、加工、汇总、存储和数据更新,实现对军事信息资源数据的有效管理。

##### 3.1.2 目录服务

目录服务用于存储、管理军事信息资源及服务资源的元数据信息,通过对元数据信息的发布、发现以及访问机制,实现数据、服务等资源的共享。通过目录服务帮助用户或应用发现分布式存储的各种军事信息资源数据。目录服务包括发现、访问和管理服务。其中,发现服务通过对元数据提供对数据资源的查找、浏览、定位功能。访问服务提供对数据级或服务级访问。管理服务提供对目录自身的管理功能,如修改目录信息、增加或删除目录等。

##### 3.1.3 交换服务

通过数据获取、数据格式转换、数据同步、交换流程控制、交换策略管理等一系列功能服务,实现数据资源的抽取、格式转换、交换过程控制、增量数据复制与同步、交换策略管理等功能服务。

##### 3.1.4 信息服务

信息服务是在目录服务基础上的数据内容服务,能提供多种多样的数据类型,能对各种空间、非空间数据及结构化、非结构化数据提供浏览、查询、下载等功能,同时为用户提供一系列的工具,帮助用户在来源众多的海量数据中进行搜索、多源数据整合、数据挖掘、辅助决策,实现军事信息资源效用的最大化。

#### 3.1.5 安全服务

信息安全服务是实现数据共享环境的网络安全、系统安全、数据安全、用户认证与授权。网络安全的内容涉及传输安全、网络边界安全、审计与监控、网管系统安全、局域网安全。系统安全主要包括物理安全、操作系统安全和数据系统安全等。数据安全需要重点考虑系统备份、容灾和恢复等内容。用户认证与授权包括用户的认证、授权、安全审计等内容。

#### 3.2 技术构架

近年来,不断成熟与完善的面向服务构架(Service-Oriented Architecture,简称SOA),以服务为导向的软件开发思想,为军事信息资源共享服务建设提供了新的途径和方法。与传统架构相比,SOA规定了信息资源间更为灵活的松散耦合关系,利用开放标准的支持,采用服务做为应用和数据集成的基本手段,不仅可以实现资源的重复使用和整合,而且能够跨越各种硬件平台和软件平台的开放标准,实现不同信息资源和应用的互联互通。

基于SOA架构的军事信息资源共享服务实现的主要思路如下。

1) 将军事信息资源从分散的各个应用系统中分离出来,按照军事信息资源共享标准进行统一的组织和服务化,成为可复用的信息资源服务。

2) 采用服务总线和适配器方式,对信息资源进行合理组织,将信息资源进行资源梳理、编目,通过目录注册和管理,便于资源使用方实现信息资源的快速定位以及管理。

3) 将应用和数据资源全部按照WSDL描述封装成服务,服务独立于实现服务的操作系统和编程语言之外,接口采用中立的方式进行定义。服务注册至服务目录中,通过不同交换服务的组合,灵活支持不同的服务模式,从而为资源共享提供全面的交换服务。通过统一的消息传送协议(HTTP/HTTPS、SMTP、RMI、FTP等),实现各交换节点间的数据互通。

4) 通过连通服务实现消息管理。

通过交换总线中的连通服务,提供多种消息交换机制,包括同步通信、异步通信模式、点对点通信模式、发布/订阅模式等,通过消息跟踪、队列管理、路由管理、协议转换实现消息通信过程中的加密、压缩、断点续传、多种通讯模式转换等重要

保障功能。

5) 通过 SOA 技术架构, 对服务提供安全、监控、维护、编排、事务机制等管理功能。同时目录的编目、发布、注册、查询、维护等功能, 都封装为服务方式, 方便扩展各种不同类型目录, 如公共

资源目录、交换服务目录、适配器资源目录等。  
基于 SOA 的数据共享环境技术构架如图 1 所示。包括: 服务资源层、交换总线层、交换服务和目录服务层、信息服务层。

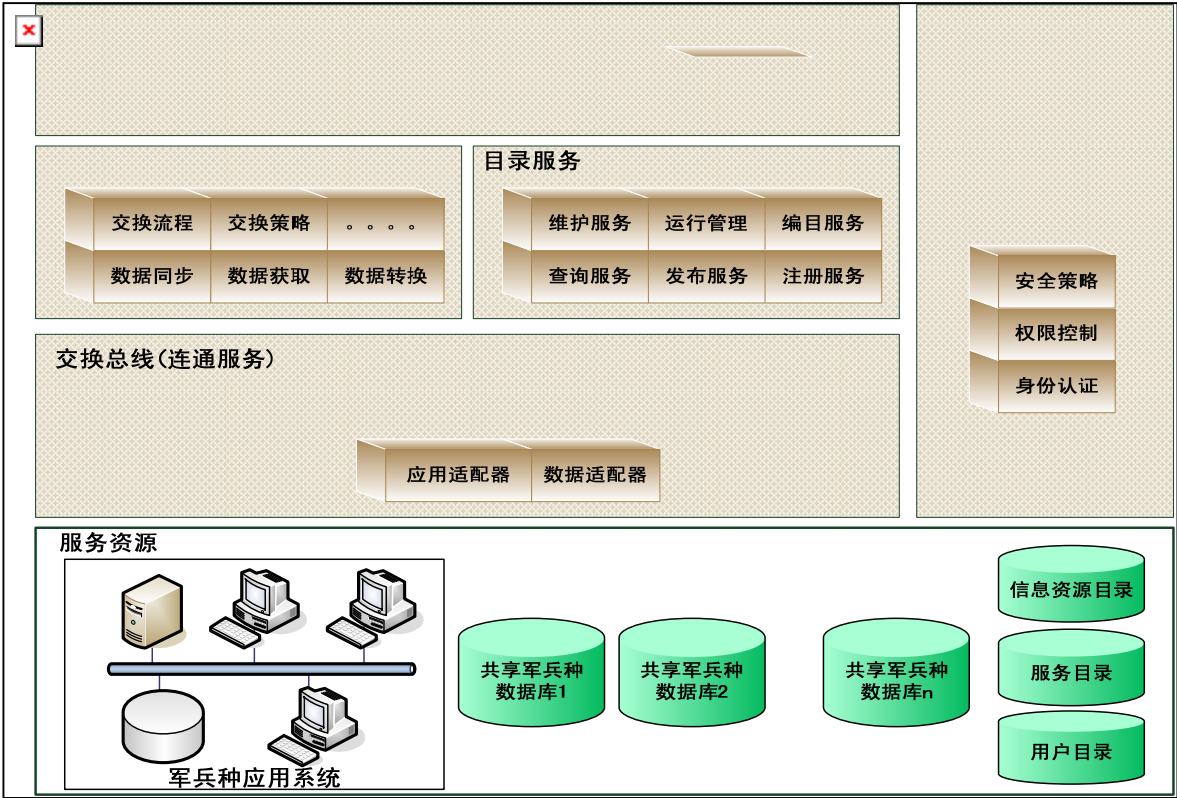


图 1 基于 SOA 的数据共享环境技术框架

4 结束语

军事信息资源共享服务体系建设是军队信息化建设的基础工程, 也是一个复杂的系统工程。需要

精心规划, 统一组织, 分工建设, 充分运用成熟、先进的信息技术, 才能实现军事信息资源的高效规范化管理与高效利用。

参考文献

[1] 刘晶炜等. IBM 信息集成技术原理及应用. 北京: 电子工业出版社, 2004.5  
[2] 王胜航等. 整合之道. IBM 中国信息支持中心  
[3] 科学数据共享工程门户网站, <http://www.sciencedata.cn>  
[4] 希赛网. SOA 专题: <http://tech.51cto.com/art/200601/16327.htm>  
[5] 赛迪网. SOA 专题: <http://tech.ccidnet.com/pub/series/s627.html>

作者联系方式

通信地址: 武汉解放公园路 45 号军事通信网建设与管理教研室  
邮政编码: 430010  
联系电话: 027-82968518/68237



# 分布式网络化作战的复杂网络模型研究

付国宾 谭海涛 沈宇

**摘要:** 从信息时代作战的角度出发, 根据复杂网络理论, 分别建立了简单、较复杂和通用的分布式网络化作战的网络拓扑结构模型, 并提出了评估该复杂网络结构模型的系统指标, 为深入认识和科学规划、优化未来一体化联合作战中各作战单元空间配置做出了有益的探索。

**关键词:** 分布式网络化作战; 复杂网络; 拓扑结构; 数学模型

## 1 引言

传统的以平台为中心的作战体系, 武器系统和传感器之间紧密耦合, 武器系统只能利用隶属配置的传感器提供的信息进行作战控制, 难以共享和充分利用其他作战资源的有用信息; 在未来以网络为中心的分布式作战环境下, 作战体系由分散部署的陆、海、空、二炮等多军兵种的传感器平台、指控平台、武器平台等作战要素融合而成, 在整个分布式网络环境中各传感器提供信息的基础上, 各类作战资源通过信息共享和平台互操作, 实现对各武器系统在作战空间部署的规划和优化从而达成最佳组合, 以高效实施对敌目标防御或攻击的作战行动, 该作战样式既符合“侦、控、打、评”的战斗过程, 也符合一体化联合作战的“兵力分散、效果集中”的作战原则, 是未来信息化战争中一体化联合作战的主要作战形式。

本文在 Watts 和 Strogatz 关于小世界网络<sup>[1]</sup>, 以及 Barabasi 和 Albert 关于无标度网络的开创性工作<sup>[2]</sup>的基础上, 力图从信息时代作战的角度出发, 建立适合分布式网络化作战的网络结构模型, 并提出评估该分布式复杂网络结构模型的系统指标, 为未来一体化联合作战中各作战单元的空间配置的规划与优化提供科学依据。

## 2 分布式网络化作战的网络结构模型

### 2.1 基本定义

现代分布式作战的战斗模型具有网络化的数学结构, 即由节点和链路构成的集合。节点是作战的基本元素, 主要包括传感器平台、指控平台、武器

平台和目标对象等。以下定义了信息化战争中分布式网络化作战节点的基本分类。

- 传感器平台 (S): 主要是指侦察机、雷达站、观通站等具有预警、侦察与监视能力的平台, 用于接收来自目标对象的可观测信息, 例如目标位置、状态、速度、航向等, 并把这些信息发送给指控平台。
- 指控平台 (C): 主要是指预警机、作战指挥所 (车、舰) 等具有指挥控制任务的平台, 用于接收来自传感器的目标监视信息和其他指控平台的指挥协同指令, 并就当前节点及将来其他节点 (平台) 的部署做出决策。
- 武器平台 (W): 主要是指战斗机、舰艇、常规导弹等具有火力攻击能力的武器装备, 用于接收指控平台的指令, 与其他节点相互作用, 并影响那些节点的状态。
- 目标对象 (T): 主要是指敌方传感器平台、指控平台、武器平台以及其他具有军事价值的节点。
- 链路: 节点间的指令或者节点间的相互作用。

对以上定义作几点说明: 第一, 节点具有敌我属性, 与 Jeff Cares 提出的节点定义不同<sup>[3]</sup>, 本文以传统的战斗过程的思路去定义节点, 此定义中传感器平台、指控平台和武器平台属性为“友军”, 目标对象敌我属性为“敌军”, 不考虑“中立”和“不明”目标的敌我属性; 第二, 目标对象不因为传感器的存在而存在, 传感器能否正确描述目标对象信息属于传感器节点内部属性, 不影响网络性能; 第三, 传感器所获得的信息必须至少经过一个指控平台, 否则可将其作为孤立点 (悬挂点) 去

除；第四，节点间的链路具有方向性，例如，传感器探测到目标信息分发给指控平台是一条链路，指控平台命令传感器任务或部署变更是另外一条链路。

2.2 简单的分布式作战网络模型

分布式网络化作战的过程可描述为：地理上分散的预警探测平台通过对目标的探测、跟踪，将空情（海情、陆情）信息分发给各作战指挥控制平台，指挥控制平台引导预先部署的精确打击武器平台对目标对象进行防御或攻击，预警探测平台对目

标损伤进行评估，并将信息分发给指控平台，指控平台决定是否对目标进行进一步的行动。

通过上面分布式网络化作战的过程描述和对网络拓扑结构中链路和节点的定义，我们可以构建一个适合分布式网络化作战的网络拓扑结构。图 1（左）描述了一个具有“敌我双方”的最简单的战斗网络，网络节点由目标对象（T）、传感器平台（S）、指挥控制平台（C）、武器平台（W）组成，实线有向线段表示信息或指令在节点间的流动，虚线有向线段表示节点间的交互作用。

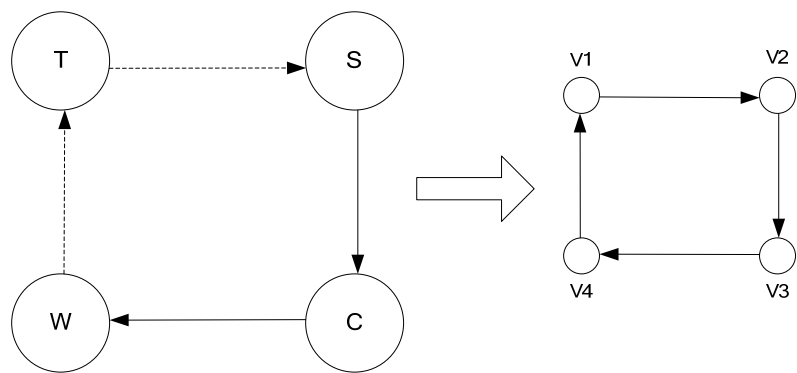


图 1 最简单的从传感器到武器平台的战斗网络

该网络可进一步抽象为一个由点集  $V$  和边集  $E$  组成的有向图  $D$ ，为简化对图的理解，虚线改为实线表示，如图 1（右）所示，设  $D = (V, E)$ ， $V = \{v_1, v_2, v_3, v_4\}$ ，节点数记为  $N = |V|$ ，边数记为  $M = |E|$ 。

为了方便对图的性能的计算，也可以用邻接矩阵的形式对有向图  $D$  进行描述。有向图  $D$  的邻接矩阵  $A = (a_{ij})$  是一个 4 阶方阵，如图 2 所示。该图描述的邻接矩阵完全等价于图 1 所描述的网络拓扑，如果不考虑节点间信息流量的大小以及节点之间的距离分布，该矩阵中“1”表示从行节点至列节点之间的一条链路，“0”表示两个节点间不存在链路（链路方向由行指向列）。

	T	S	C	W
T	0	1	0	0
S	0	0	1	0
C	0	0	0	1
W	1	0	0	0

图 2 最简单的分布式网络作战的矩阵表示

这是一个最简单的分布式网络化作战模型，而实际作战可能包含更多的目标对象、传感器平台、指控平台、武器平台以及不同类型的链路，并且两个节点间甚至有多条链路。下面以一个较复杂的分布式网络来描述分布式网络化作战的功能。

2.3 较复杂的分布式作战网络模型

在分布式网络化作战体系中，任何一次作战斗都是将传感器网络、指控网络、武器网络相互协作的过程，来自于不同逻辑功能网络的功能节点（平台）根据具体作战的需要，临时形成一个由多个信息环路组成的面向作战任务的分布式网络化架构，如图 3 所示。

在环 S1-S2-C1-C2 中，指控平台 C1 控制着传感器 S1，传感器 S2 同时从 S1 和目标对象 T 获取信息，并将信息报告给指控平台 C2，指控平台 C1、C2 之间进行作战任务的指挥控制协同，C1 可以命令 S1 接近目标对象 T，以便进行更好的观测，从而形成一个对传感器的控制环路。在环 C1-C2-W1-W2-T 中，C1、C2 分别指挥控制武器平台 W1、W2 对目标 T 实施空中拦截与攻击。该面向

作战任务的分布式网络中实现的功能群组主要有：情报报知（态势感知）群组、指控协同群组、指挥引导群组、武器协同群组等，这体现了分布式网络化作战中形成的逻辑功能网络的雏形。

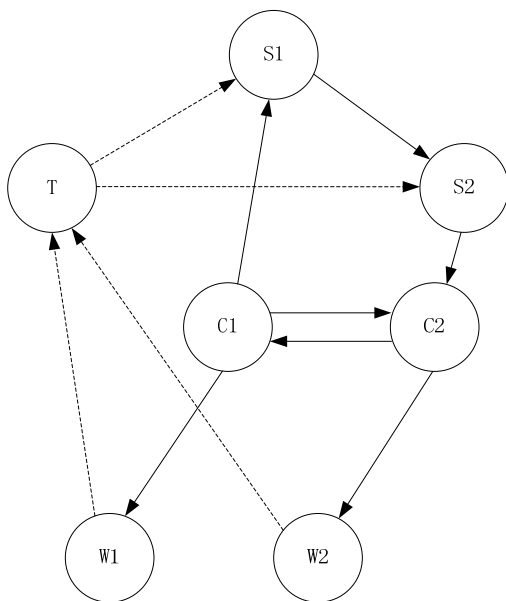


图3 较复杂的分布式作战网络模型

	$T$	$S_1$	$S_2$	$C_1$	$C_2$	$W_1$	$W_2$
$T$	0	1	1	0	0	0	0
$S_1$	0	0	1	1	0	0	0
$S_2$	0	0	0	0	1	0	0
$C_1$	0	1	0	0	1	1	0
$C_2$	0	0	0	1	0	0	1
$W_1$	1	0	0	0	0	0	0
$W_2$	1	0	0	0	0	0	0

图4 较复杂的分布式网络的邻接矩阵表示

该网络（有向图）也可以用邻接矩阵来表示，如图4所示，该邻接矩阵同样描述了网络中所有节点中两两之间的交互关系。这样一个较复杂的分布式网络化作战网络模型完成了信息化战争条件下的“侦、控、打、评”的战斗循环过程，但是这样的二维图形的表达方式只考虑了节点之间的连接关系，掩盖了分布式网络化作战的复杂性。

## 2.4 分布式网络化作战通用网络模型

假设一个网络含有  $m$  个目标对象， $n$  个传感器平台， $p$  个指控平台， $q$  个武器平台，不考虑节点间的信息流量大小，只考虑节点间的交互关系，其

构成的分布式网络化作战体系的网络拓扑结构可由邻接矩阵  $A = (a_{ij})$  来描述，该矩阵为  $N \times N$  阶矩阵。其中， $N$  为组成网络的节点数量： $N = m + n + p + q$ ， $L$  为链路数量：

$$L = \sum_{i=0}^N \sum_{j=0}^N a_{ij}。$$

用邻接矩阵描述分布式网络化作战的网络模型具有一定的通用性和可行性。例如，假设  $n$  个传感器平台组成传感器网络、 $p$  个指控平台组成指控平台网络、 $q$  个武器平台组成武器平台网络均是全连网络，整个网络可看作是支撑网络中心战（NCW）的全球信息栅格（GIG）；若假设传感器数量、指控平台数量、武器平台数量均为1，即构成最简单的战斗网络；如果做进一步简化，把传感器、指控平台、武器平台及目标合并成一个对象，将单兵表示成一个含有传感器、指控器、武器的集合点，可将交战网络看作单兵间的对抗。然而，分布式网络化作战的网络化作战效能依赖于大量节点（平台）的存在，通常来讲，一个节点少于50的网络不会产生显著的网络化作战效能。具有大量节点的分布式作战网络是异常复杂的，通常一个具有方向性的  $N \times N$  阶矩阵可以构造出  $N \times (N-1)$  条有向链路，即使  $N$  值很小，网络包含的子网数量以及链路数量也非常巨大。虽然在实际的作战模型中不会两两节点之间都有链路，但在分布式网络化作战的交战网络中绝大多数情况下还是包含数十个、上百个，甚至上千个节点，所以其复杂性仍然很高。

在如此庞大的状态空间中，试图找到一种节点和链路的最佳组合将是一件极其复杂的工作。利用邻接矩阵建立分布式网络化作战的通用网络模型，并对该矩阵进行计算与分析，可研究传感器数量、指控平台数量、武器平台数量以及平台间的交互关系对分布式网络化作战的网络效能的影响。那么，如何科学评价分布式网络化作战的复杂网络效能呢？

## 3 分布式网络化作战网络模型的评估指标

近年来针对因特网、万维网、社会网等问题的研究，对复杂网络系统的结构及演化特性有了

新的认识,主要的研究成果是在刻画复杂网络结构的统计特性上提出了许多概念和方法。根据这些研究成果,结合分布式网络化作战的特点,下面提出几个基本的概念作为度量指标:链路节点比、度分布和集群系数,这些特性可作为信息时代分布式网络化作战复杂网络模型分析和试验的简明准则。

### 3.1 链路节点比

支撑美军“网络中心战”的全球信息栅格,要求网络为最大连通度网络,所有节点都与其他节点直接相连,通过计算可得出最大连通度网络的链路节点比为  $M/N = (N-1)/2$ ,考虑到链路的方向性,则链路节点比  $M/N = N-1$ ,这显然将导致大量不必要的开销。而在关于复杂网络的研究中发现,只需要少得多的链路就可以使网络获得非常好的连通度,而且在一个链路节点比小于最大连通度的网络中,网络的路径长度、局部凝聚度、顽存性和自适应性等参数仍然可以有比较理想的数值。有文献指出,当链路节点比  $M/N$  大约为 2 时,所有这些特性就会表现得相当优异<sup>[1]</sup>,而最脆弱的结构——链状网,其链路节点比约为  $N-1/N$ ,  $N$  非常大时,链路节点近似取值为 1。这说明,分布式网络化作战的网络拓扑结构并非需要是一个全连通的网路,当链路节点比大约为 2 时,则只需要在最简单的链状网上再增加一倍的链路即可获得较好的网络效能。

### 3.2 度分布

节点的度分布是指网络中度为  $k$  的节点的概率  $P(k)$  随节点度  $k$  的变化规律。节点  $i$  的度定义为与该节点相连的其他节点的数目。有向网络中一个节点的度分为出度和入度,节点的出度是指从该节点指向其他节点的边数,节点的入度是指从其他节点指向该节点的边的数目,节点的出度和入度可通过相对应的邻接矩阵的计算获得<sup>[5]</sup>。一个节点的度越大就意味着这个节点在某种意义上越重要,指控节点的出度和入度都较大,对网络具有重要意义。分布式网络化作战的网络同因特网一样可看做是无标度网络,服从幂律分布形式  $P(k) \propto k^{-\gamma}$ ,幂律分布在是对数坐标系中对应于一条直线,是一个自适应复杂网络,为实现网络的自适应特性,链路不应该被均匀的分布在网络当中。网络应该有非常少量的

高连接度节点,中等数量的中等连接度节点,大量的低连接度节点。同时,无标度网络具有对随机故障的鲁棒性和恶意攻击的脆弱性,这种“鲁棒而又脆弱”的特性要求分布式网络化作战中的指挥控制节点,需要具有高度的稳定性,这对整个系统的稳定性起着关键性的作用。

### 3.3 集群系数

集群系数 (Clustering coefficient) 反映网络的群集程度,定义为网络的平均度与网络规模之比,记作  $C = \frac{\langle k^2 \rangle}{N}$ 。显然,  $0 \leq C \leq 1$ 。 $C = 0$  时,所有节点均为孤立节点,  $C = 1$  时为全连通网络,对于完全随机的网络,当  $N$  很大时,  $C = O(N^{-1})$ 。许多大规模的实际网络都具有明显的聚类效应,分布式网络化作战的网络拓扑结构也应该具有此特征,即  $N \rightarrow \infty$  时,集群系数  $C$  可近似为一个常数,  $C = O(1)$ ,类似于社会关系网络中的“物以类聚,人以群分”的特性。分布式网络化作战的网络可以根据聚类系数的大小分成若干个群组,在这些群组内部的连接较为紧密,但是,各个群组之间的连接却较为稀疏。例如,由传感器平台形成的传感器群组,由武器平台形成的武器群组,由面向作战任务的作战任务群组,我们得出,群组内中的所有节点并非都需要与群组外节点发生相互作用,找到并分析这些群组,有助于我们更好地理解分布式作战网络的全局行为,根据网络节点自群的空间分布来优化调整作战资源。

以上这些指标或准则是从其他领域的复杂网络研究中推断出来的特征,在军事网络中完全有可能得出不同的数值。同时,这里仅仅是模型的拓扑度量方法,实际网络中的节点和链路并不是这样简单的二元连接关系,而是有着更加复杂的赋值,需要将以上所列出的所有这些特性应该综合起来,建立基于变化的环境、动态的节点链路来描述完全自适应分布式网络化作战的行为特征,进一步研究简明准则的细化问题。

## 4 结束语

分布式网络化作战是信息时代战争的主要作战形式,对该作战体系的网络拓扑结构的研究是一个异常复杂的问题,其数学模型的构建是一个复杂的

系统工程, 对其深入研究对我军实施一体化联合作战体系的总体设计、作战资源高效利用具有重要的意义。论文在建立分布式网络化作战的拓扑结构数学模型基础上, 进一步提出了评估该复杂网络结构的系统指标, 对一体化联合作战的作战单元的空间配置优化和网络效能评估具有科学的指导意义。建

立的拓扑结构数学模型都对作战进行了简化, 没有考虑节点间的信息流量以及节点在空间上的具体分布, 只有对网络节点、链路的权值赋值, 才能更好地描述分布式网络化作战的实际情况, 这需要进一步深入研究。

### 参考文献

- [1] Jeffrey Cares, Distributed Networked Operations The Foundations of Network Centric Warfare, [M], 2006 October.
- [2] Watts D J, Strogatz S H. *Collective dynamics of 'small-world' networks*. Nature. [J]1998
- [3] Barabasi A L, Albert R. *Emergence of scaling in random networks*. Science. [J]. 1999
- [4] 毛昭军. 网络化防空导弹体系虚拟拦截联盟研究, 军事运筹与系统工程, [J], 2007 年第 1 期.
- [5] 肖位枢. 图论及其算法[M]. 北京: 航空工业出版社, 1993 年 7 月.:20—38

### 作者联系方式

通信地址: 武汉解放公园路 45 号通信指挥学院 20 队

邮政编码: 430010

联系电话: 13397190100 0781-190100

# 多星遥感任务规划体系框架构想

郭建恩 陈健 李湘 王鹏

**摘 要:** 本文根据多星遥感任务规划的需求, 从任务规划的业务架构、信息流程、系统架构和技术架构四个方面对任务规划的体系结构进行了研究分析, 提出了可行的方案, 为多星遥感任务一体化规划提供了可行的思路。

**关键词:** 空天一体化; 多星遥感; 任务规划; 体系结构

## 1 前言

在多星遥感任务规划方面, 无论是理论研究还是实际应用来说, 美军无疑是代表了最高水平。美国很早就通过军方研究机构(美国空军实验室、海军实验室)、民间研究机构(美国喷气实验室等)和一些大学(加州大学等)联合开展研究工作, 其研究成果已经应用于经济和军备建设中。通过美国在波黑战争、海湾战争和阿富汗战争中所展现的航天遥感信息保障能力来看, 美国已经具备了多类型卫星联合实施航天遥感的能力。

但是由于保密的关系, 国外有关多星遥感任务规划问题的资料很难获取。从目前检索到的资料来看, 只能获取少数关于多星调度的问题, 并且都只是针对某一方面或者某些方面进行遥感受物调度, 没有考虑全面。如美国弗吉尼亚大学的 S.BurrowBridge 和美国国家航空航天管理局的 Al.Globus 和 J.Frank 等人从理论上探讨了多颗对地观测卫星调度问题; BurrowBridge 讨论了如何单纯针对地面测控资源进行优化分配; Globus 等讨论了一般的多颗对地观测卫星调度问题。关于多星遥感任务规划体系架构的设计和讨论目前还无法检索到相关资料。

随着我国航天遥感事业的发展, 我们正在逐步摸索多星遥感任务规划的体系结构、优化算法等各个方面问题。

本文从四个方面研究多星遥感任务规划的体系框架。

1) 业务体系结构: 以遥感任务的建模、规划、调度等应用流程为基础进行研究。

2) 系统体系结构: 从多星遥感任务规划系统软件平台、资源构成、节点结构等方面进行研究。

3) 技术体系结构: 从多星遥感任务规划系统所采用的技术路线来研究其构成。

4) 工作流程和技术流程: 从多星遥感任务规划系统的工作流程和技术流程来研究。

## 2 多星遥感任务规划业务体系

多星遥感任务规划体系结构的业务体系主要从应用需求的角度出发, 描述基于多星遥感任务规划系统的应用流程, 划分应用层次, 描述各部分之间关系。

根据我国某遥感卫星地面应用系统多年运行经验, 结合多星遥感任务规划系统应用流程(用户请求→生成遥感需求订单→遥感任务建模与分析→遥感资源分配→综合任务规划→规划结果仿真检验与评估)。多星遥感任务规划系统业务体系设计为 6 层结构, 在此体系中, 上层可以调用下层的功能和服务, 形成了从任务信息获取、传输到管理、资源配备、应用的完整体系(如图 1 所示)。

从业务逻辑的角度将多星遥感任务规划系统共分为六层。依次为: 基础数据层、数据服务层、模型层、业务功能层、业务平台层、应用系统层。各层之间, 下层为上层提供特定的服务和业务支持, 保证上层系统的正常运行。最底层的基础数据层负责对基础数据(如卫星轨道信息、数传资源信息、遥感任务数据、气象数据等)的获取、存储。数据服务层对数据层中各数据进行封装, 并对基础数据进行维护, 同时为模型层提供数据查询服务。模型层是业务功能层的基础, 包括资源模型、任务模型、规划模型、仿真模型等, 对应了业务功能层的各个方面的需求。模型层对数据的需求由数据服务层满足。业务功能层为业务平台提供相应的业务功

能服务。业务平台层依据业务功能层提供的相应服务，为应用系统层中应用系统提供平台支持。应用系统层为各用户单位提供多星遥感服务，并对遥感任务进行仿真，对遥感结果进行评估。

### 3 多星遥感任务规划系统体系结构

多星遥感任务规划系统的系统体系主要描述多星遥感任务规划系统平台和资源节点的结构，多星遥感任务规划系统的系统体系由三大部分组成：多星遥感任务和资源建模、星地一体化规划调度平台和仿真评估与结果输出（如图 2 所示）。其中，遥感资源是指多星遥感任务规划系统中的各个遥感卫星（包括可见光卫星、SAR 卫星、电子卫星、海洋卫星等）、用于向卫星注入遥感指令和接收下传数据的地面站、系统软件系统、系统网络资源、数据信息等，这些资源将通过多星遥感任务规划系统的规划调度统一提供给资源请求者（申请遥感任务的各个用户）使用。遥感资源任务建模将各个用户单位提出的遥感任务进行一定的抽象，用统一的模型进行描述，以便多星遥感任务规划系统任务分析调度平台结合现有可用资源进行相应的资源分配和调度。星地一体化规划调度平台主要由遥感任务分析、区域覆盖、复杂任务规划调度、星地一体化规划调度、动态任务调整调度、仿真评估与结果输出模块等功能软件组成，通过一体化的遥感资源管理，对遥感资源实行合理分配。在此基础上，各种遥感资源的分配和调度（如遥感任务分析处理、遥感数据获取等）得以实现。

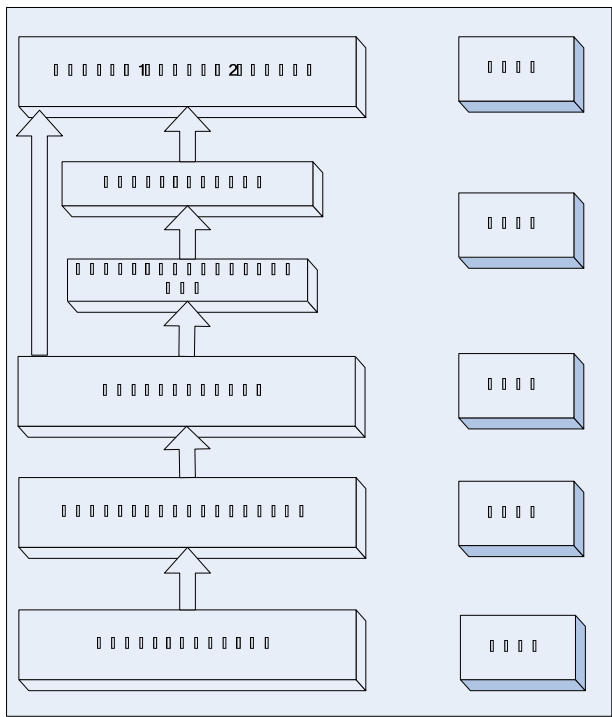


图 1 多星遥感任务规划系统业务体系结构图

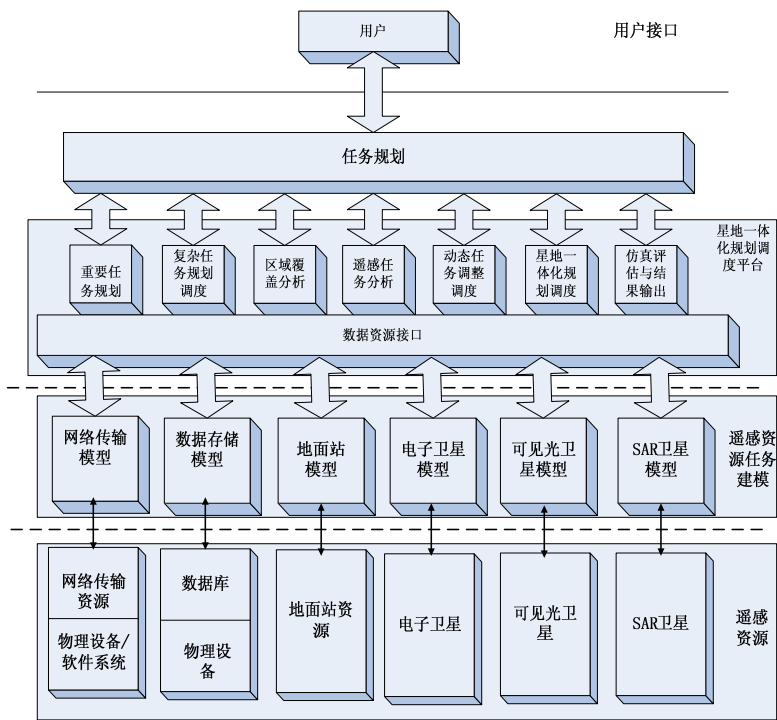


图 2 多星遥感任务规划系统的系统体系结构图

4 多星遥感任务规划技术体系

多星遥感任务规划系统的技术体系是指由贯穿各种卫星信息获取、多星遥感任务和资源的统一建模、多星遥感条件下复杂任务的分解算法、强时效性条件下的快速遥感任务规划、星地一体化任务规划模型和算法、联合任务规划的仿真检验和定量化评估等一系列技术所构成的一组完整的技术方法的总和，它是实现多星遥感任务规划系统的技术保证。

多星遥感任务规划系统技术体系的建立依赖于许多基础理论和相关前沿技术的研究，多星遥感任务规划系统技术体系分为基础技术和关键技术。多星遥感任务规划系统基础技术主要包括专家决策支持系统技术（包括遗传算法、模拟退火算法、禁忌搜索算法等）、运筹学规划技术（包括线性规划技术、非线性规划技术，组合优化技术）、遥感与测

控技术、GIS 技术、系统建模与仿真技术、卫星应用技术、指挥自动化技术等。而多星遥感任务规划系统关键技术主要与遥感卫星应用和处理的整个流程相对应，着重在遥感任务采集、建模，传输、资源获取、资源建模、组织管理、分析处理、应用等各个阶段和层次上解决各遥感卫星资源共享和协同工作的技术问题，包括遥感任务的数学描述机制与资源需求转换模型技术、遥感资源的使用约束与分配规则的建模与表达技术、多星遥感条件下的复杂区域高效覆盖算法、卫星访问信息快速计算算法、有效遥感资源的快速查询算法、强时效性条件下的遥感计划快速编制算法、遥感数据的快速联合接收算法、任务规划的动态优化调整算法、星地一体化资源调度与规划技术、多类型遥感任务规划的模型和优化算法、任务规划的仿真检验技术、任务规划的定量化评估等技术。多星遥感任务规划系统技术体系如图 3 所示。

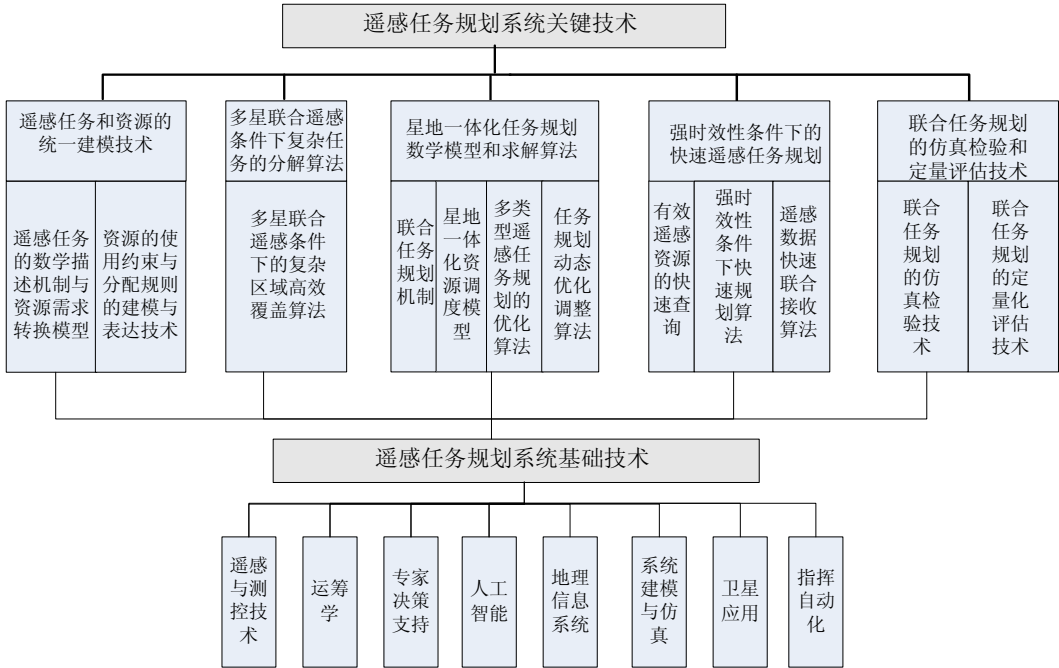


图 3 多星遥感任务规划系统技术体系结构图

5 多星遥感任务规划流程

5.1 工作流程

多星遥感任务规划的主要任务是根据遥感任务请求，合理分配卫星以及地面站资源，使得资源利用率最大化，以获取尽可能多且重要的遥感数据。具体言之，就是根据卫星有效载荷能力和地面站接

收能力，以及遥感约束条件，合理分配各个卫星的遥感任务请求，并且通过合理分配地面站，实现卫星遥感数据的快速接收。

多星遥感任务规划的工作过程具体如下。

- 1) 根据各星的星下点轨迹以及侧视角度，获取各星可观测的地面目标。
- 2) 根据请求信息或者用户信息获取各目标对传感器的具体需求。



3) 根据传感器类型、分辨率、气象条件等约束,剔除卫星无法观测的目标;将不可能被多颗星观测的目标分配给各个卫星。

4) 将没有时间冲突的地面站接收资源分配给各个卫星。

5) 对于满足多颗星观测条件的目标,根据目标性质、请求类型等确定是否可以多星观测。例如,如果是普通目标,则只安排一颗观测效果最好、有利地面站接收的卫星观测,如果是重要目标,则允许多颗星重复观测。

6) 对于只要求被单星观测的目标,根据各星的任务状态、地面站状态、传感器类型等进行决策分析,消解多星观测冲突,将目标分配给确定的单颗星。

7) 在分配好各星的观测任务后,根据各星的存储器大小、分辨率、下传速率等特点,合理分配地面站数据接收任务,尽量保证各星所获取的数据能够有效下载到地面站进行处理。

8) 根据分配的地面站的各星的遥感任务进行修订。

9) 对任务规划结果进行仿真显示。

## 5.2 技术流程

### (1) 任务数据获取综合

任务规划首先获取每颗参与规划卫星在任务规划时段内的可访问目标列表、针对每个参与规划地面站在任务规划时段内的跟踪接收时间段、当前未完成的遥感任务安排单以及相关的辅助规划信息等输入数据。

针对获得的上述输入数据,提供可视化调整模块,显示任务时间段、参与卫星资源与载荷能力信息、涉及地面站系统资源信息、用户信息、目标统计信息及其具体参数信息等,允许用户对参与卫星进行选择,对卫星参数、地面站资源、遥感请求等级等相关参数进行修改调整。

### (2) 任务分配预处理

任务分配预处理初步完成目标与地面站的分配,主要包括以下几个方面。

(a) 资源和约束条件修正:由于实际情况某些原因导致某些理论资源无法分配或正常使用,需要在分配任务之前进行资源和约束条件的修正处理。

(b) 约束过滤:根据卫星遥感约束、卫星载荷

实际工况,过滤不满足条件的遥感任务目标。

(c) 用户需求处理:根据用户的需求信息(关心的地域、关心目标的类型、需求的频度、需求迫切性等)特点、任务请求类型等,确定具体的遥感要求,包括分辨率、时效、传感器类型、频度等,据此对每颗卫星的可遥感目标列表进一步过滤,使得每颗卫星的遥感任务列表内的目标都能满足用户的需求。如果输入的任务信息中已经具有了非常明确的遥感要求,如传感器类型、分辨率等,则直接根据要求进行过滤。

(d) 目标与地面站预分配:根据由用户需求信息、任务请求类型等信息确定的具体遥感要求,结合实际资源和约束条件,对经过过滤的任务进行处理,具体确定出每个满足约束的目标所用的卫星及其传感器、每个卫星数传所用的地面站及其回放时间段列表。

### (3) 冲突消解决策

(a) 考虑目标对应的用户信息,如果用户需求紧迫程度较高,则下一个地面站访问时间距目标访问时间最近的卫星优先分配到该目标。

(b) 如果用户需求频度较高,则访问该目标的每颗冲突卫星均得到该目标的遥感任务。

(c) 根据观测效果因素确定规则:如果是光学卫星,则考虑拍摄效果条件尽可能好,优先分配太阳高度角较大、云量覆盖较少的卫星拍摄;如果是SAR,红外等类型的卫星,则根据判定的拍摄效果确定。

(d) 根据星上载荷限制确定以下规则:如果某冲突目标的观测卫星中,一颗卫星的传感器类型只有一种,而另一颗卫星的传感器类型有多种,则优先分配目标给传感器类型少的卫星。

(e) 考察目标分布进行相关计算,确定下列规则。

- 以目标为中心,长度为卫星最短拍摄时长,宽度为该星最小视场角范围内的目标数目多的(可以是一个比值问题,因为可能都很多;可维护一个阈值管理,比如一个是另一个的一倍以上的认为是较多)卫星优先获得该目标的遥感任务;
- 与该目标在同一拍摄时段内,不在以该目标为中心的视场角内的目标数目少的优先分配该目标;
- 已分配目标中重要目标数目少的优先分配;

- 已分配目标数目与卫星存储容量的比值小的优先分配。

(f) 对于满足多颗星的观测条件的目标, 根据目标性质、请求类型等确定是否可以多星观测。例如, 如果是普通目标, 则只安排一颗观测效果最好、有利地面站接收的卫星观测, 如果是重要目标, 则允许多颗星重复观测。

(g) 冲突消解决策解决目标与地面分配中可能出现的冲突, 主要包括:

- 目标分配冲突消解: 根据各种约束条件及观测要求确定每颗参与任务规划的卫星的可观测目标以及解决可被多颗卫星观测的目标的冲突;
- 地面站分配冲突消解: 相对于每颗卫星的地面站可接收时段, 为每颗卫星分配地面站接收时段任务, 并解决不同卫星对地面站资源的需求的冲突。

#### (4) 可视化决策

(a) 人机交互调整: 把上述决策结果进行可视化显示, 提供示意图(或实际地图)和图表两种表示方法, 提供规划解释和统计分析, 允许操作人员调整修改规划结果。

(b) 约束检测: 对上述决策结果进行冲突检

测, 检测出不满足约束条件的遥感任务(目标)或数传任务(地面站), 并提供可视化界面由人工解决冲突。

#### (5) 任务规划结果生成

根据冲突消解和决策结果, 生成针对单星的遥感任务定单, 包括确定的分配给其的遥感任务请求和地面站接收资源信息, 具体卫星的计划管理系统据此编制各自的计划。

#### (6) 联合任务规划结果定量化评估

针对任务规划方案中规划结果合理性、遥感资源的合理使用以及目标的安排情况等, 研究遥感任务规划结果的评估模型和相应的评估算法, 对任务规划产生的遥感途径合理性做出定量化评估。

## 6 结束语

本文从业务体系结构、系统体系结构、技术体系结构、工作流程和技术流程四个方面对多星遥感任务规划的体系框架进行了初步构想和研究。研制多星遥感任务规划平台, 对于整合多星遥感资源, 充分发挥其遥感效益具有重要意义。

## 参考文献(略)

## 作者联系方式

通信地址: 北京清河小营东路2号院61646部队

邮政编码: 100085

联系电话: 13911228015

# 军事信息系统综合集成研究

胡双喜 汤怀松 金家才

**摘 要:** 本文主要对我军军事信息系统中装备信息系统、情报侦察信息系统、指挥控制信息系统和综合保障信息系统综合集成的要点进行了初步的研究。

**关键词:** 信息系统; 综合集成; 军队

军事信息系统是联接全军作战单位和作战平台的神经网络,任何作战行动都要依赖军事信息系统。军事信息系统的结构是否合理,运转是否顺畅,将直接影响作战效能的发挥。军事信息系统主要由武器装备信息系统、情报侦察信息系统、指挥控制信息系统和综合保障信息系统四个部分构成。军事信息系统的综合集成是指按照一体化联合作战的要求,在综合集成技术的支撑下,将作战体系中的武器装备、情报侦察、指挥控制、综合保障等信息系统进行科学安排和优化组合,建立起作战系统、体系内部的有序结构,使其能够充分发挥各个信息系统的效能,达到“整体大于部分之和”的效果。

## 1 武器装备信息系统综合集成

武器装备信息系统综合集成是军事信息系统综合集成的前提和基础。武器装备信息系统的综合集成建设要根据未来一体化联合作战的需求,重点把握以下三个方面。

### 1.1 武器装备的数字化

武器装备的数字化是武器装备信息系统综合集成的基本条件。1996年出台的美国“数字化总计划”指出,“数字化是一种极为关键的力量倍增器,……将提供打赢各战役所需要的信息”。我军武器平台的数字化建设应当采取改造与研制相结合的方法。一方面,是对现役的武器装备进行数字化改造,如对旧装备加装信息系统、指挥员综合显示器、全球定位系统等数字化设备。另一方面,加紧研制具有“嵌入式”数字化能力的新一代武器装备。嵌入式系统的开发和应用是研制新一代武器装

备,实现武器装备数字化的主要途径。

### 1.2 武器装备的标准化

武器装备的标准化是一体化联合作战对武器装备信息系统需求的重要内容。“通用化”、“系列化”和“模块化”是标准化的三种形式。武器装备的通用化是指对武器装备普遍采用标准化的模块结构,通过组建多种作战平台通用的弹性系统骨架,使不同的系统、设备之间尽可能拥用相同的电子模块,相互之间可以通用,根据不同的作战对象快速组装成功能不尽相同的武器装备。武器装备的系列化是指根据某种武器装备的使用需求和发展规律,按一定数列合理排列或统一其主要性能参数、结构形式,有目的地指导该类装备的发展,以满足广泛需求的一种标准化方法。模块化是对某类设备或装备,在进行功能分析和分解的基础上,划分并设计、生产出一系列通用模块或标准模块,然后从中选取相应的模块,并补充新设计的专用模块和零部件,组合成不同的新设备或新装备,以满足各种需求的一种标准化方法。武器装备的“三化”都是建立在继承性原则和互换性原理之上的,有着不可分割的关系。在武器装备的标准化建设过程中,要综合运用“三化”。

### 1.3 武器装备的功能集成化

高新武器发展过程中,以往那种功能单一、型号复杂的现象正在发生根本的改变。80年代以来,国外武器装备发展的总趋势是走基本型派生发展的道路,实现“一机多用”、“一机多型”。武器装备的多功能化受到各国军方的普遍重视。武器装备的功能集成化是指将功能相近、相互关联的数个设备组合成一个系统,从而简化系统,实现资源共

享,提高武器装备的信息综合能力和快速反应能力,同时对付多种威胁。在未来武器装备发展上,要从注重特定的单一用途转向强调一专多能,在提高性能、质量的同时,注重减少型号品种。

## 2 情报侦察信息系统综合集成

情报侦察信息系统的综合集成是指在一体化通信网络支持下,将情报信息中心、各类情报侦察力量组合在一起,加入地面、海上、空中、空间等各类传感器,以及能产生情报信息的仿真作战实体,构成一体化情报信息系统。通过对各类作战信息的探测、传输、处理和分发,实现战场信息的顺畅流动和信息传输的无缝链接,实时准确生成战场态势图,并从信息的有效分发与使用中获得行动优势。

### 2.1 建立综合情报信息处理中心

未来信息化作战,情报信息中心的主要任务是统一筹划和组织所属情报信息力量的运用,综合已有情报信息,生成一组战场通用态势图,为情报用户提供各种信息服务。因此,情报信息中心应具有情报信息的自动处理、分发、管理和信息共享等功能。构建综合情报信息处理中心的应当把握以下几点:一是构建综合情报信息数据库。首先由各信息作战单元情报处理中心对信息进行融合处理,建立包括敌、我、友、战场环境等要素的基础数据库;其次由联合信息作战情报处理中心对基础数据库信息进行再次融合处理,通过分析判断、对比、识别,消除冗余信息,统一格式,建立综合情报信息数据库。二是提高情报处理自动化程度。更新情报处理计算机硬件,提高系统运行速度;配套情报自动处理设备,完善情报处理手段;升级情报处理软件,提高战场情报信息的自动融合处理能力,实时生成态势图,实现情报处理的自动化。三建立侦察情报分发子系统。研制情报自动分发软件,建立人工和自动分发网络,实现情报信息的按需分发;广泛采取电子邮件、数据通信、专向广播、有线电话、视频传输等多种周端,实时向指挥员和各情报终端提供信息,实现共享。

### 2.2 整合情报侦察力量

整合情报侦察力量主要是指打破战略、战役、

战术和各军兵种不同级别的情报侦察力量条块分割、自成体系的力量结构,依托战场一体化信息网络,将各种情报侦察力量联结成一体化情报侦察网,由情报信息中心统一计划,各级分头管理,达成信息共享。情报侦察力量整合的目的是:通过融合多种情报源对同一目标的探测结果,提高探测精度;通过对多种渠道获得的情报进行互相印证,保证情报信息的真实准确;通过动态任务分派,指定某一情报源专门探测某一目标或某一方向,提高探测效率。具体做法如下:① 专门的信息作战情报侦察力量(如雷达和通信侦察营、连、站等)及人民群众侦察力量,为情报信息中心和本级部队提供双重信息服务;② 与武器平台直接相连的侦察探测力量(如炮兵前方观察哨、炮瞄雷达、校射雷达、目标搜索雷达等),在保障武器平台作战的同时,向情报信息中心实时发送所获情报信息;③ 各军(兵)种作战部队作为一类情报信息力量,也应依托一体化信息网络及时发布己方的有关信息(如位置、状态、企图等),以及相关的敌情和双方作战态势等信息。

### 2.3 实现情报信息链的网络化

情报信息链的网络化包含两方面的内容:一是缩短情报信息流程,即将情报收集信息链调整为情报实体→作战单元情报侦察控制中心(各群或分群指挥所)→联合信息作战情报中心三层节点,情报分发信息链调整为联合信息作战情报中心→情报用户两层节点。情报信息流程的改进,使情报信息传递层次大幅压缩,流速明显加快,流量显著增加,获得情报信息更多更及时的作战实体可以更好地了解战场态势,更快地做出反应。二是变树状结构为网状结构,即实现各作战单元情报侦察控制中心的互联互通互操作。网络结构的形成,使得各横向作战单元可以共享情报信息资源,为作战行动提供大量的及时的情报支援;提高了情报信息链的抗毁性,如对于某个信息作战单元来说,在其纵向信息链被毁的情况下,仍然可以通过其横向迂回链路来保持信息指令的畅通。

## 3 指挥控制信息系统综合集成

指挥控制信息系统综合集成是指在一体化通信

网络支持下,将作战单元的各级指挥所及所辖具备入网能力的各级指挥机构,融入各级指挥自动化系统,构成一体化指挥控制系统。指挥控制信息系统综合集成的主要目的是通过综合集成达成战场态势实时共享、分布式任务规划与协调决策、实时作战评估的目的,实现各种指挥控制信息顺畅流动和近乎实时的指挥控制。

### 3.1 指挥机构合成精干化

首先,要提高指挥机构的合成程度。只有结构上的合成,才能有功能上的融合。因此,在编组一体化联合作战指挥机构时,指挥员、副职指挥员及各职能部门主要负责人应由不同军种人员分别担任;参谋人员应按一定比例由各军种机关有关人员组成。其次,要科学设置指挥机构和人员编成,力求精干。应着眼联合作战指挥的需要,削减冗员,调整机构和人员配备,压缩减少不必要的部门,合并职能雷同的部门,撤消与作战无关的部门;增编联合作战指挥紧缺的部门,实现信息作战指挥机构与指挥功能相匹配。另外,精干的含义还应包括指挥人员素质方面的要求。就是说,在精简信息作战指挥机构人员数量的同时,要提高指挥人员业务素质,既要精通指挥业务,又会熟练使用指挥自动化系统,同时也会科学处理信息,力求做到一专多能,指挥合一,具备计划和组织指挥一体化联合作战的能力。

### 3.2 指挥手段精确高效化

未来信息化战争中,战场环境的全维感知要求指挥控制手段必须精确高效化。机械化时代的战场,由于获取信息的器材和手段有限,加之“树状”指挥控制结构使信息传输的层次多、渠道不畅、信息流转时间长,指挥员很难把握信息的实时性效应。指挥控制主要趋于对“势”的把握,对“面”的打击与控制,是基于“决策--打击”的指挥控制模式。在未来联合信息作战中,应当依托遍布全球下至深海、上至太空的传感器网,跨越延伸到所有作战单元、要素,实时共享态势感知,为各个层次,各个级别同步提供通用作战图像和第一信息,增加指挥员对战场的感知度,实现战场有利于己方的“单向透明”。使得指挥员能够依托指挥信息网络,充分发挥人机互动决策支持系统的巨大优势,实现指挥员的主观意志与精密的定量计算、定

量分析、实时反馈有机结合。实现指挥控制以往对“面”的概略打击与控制向对“点”的精确打击与控制的转变,并在精确的时间和地点科学地部署和使用兵力火力,精确地指挥控制到单兵、单件武器平台,形成基于“引导(信息)--决策--打击--反馈--决策--打击”精确高效的指挥控制模式,最优、最大地发挥各种作战力量的战斗潜力。

### 3.3 指挥体制扁平网络化

过去,我军指挥体制普遍采用“上下相连、互邻不通、纵长横窄”的“树”状结构。这种指挥体制虽有利于上情下达、下情上报,但随着信息技术的飞速发展及其在战争中的运用,其弊端已日渐突出:同级单位之间、侦察系统与武器系统之间不能横向沟通,战场信息必需经上级层层中转,这就导致信息流程长,传递速度慢;抗毁力差,被切断“一枝”,就影响一片;切断“主干”,则全部瘫痪。近年来的几场高技术局部战争已经证明:“树”状指挥体制已越来越不适应世界军事发展和军队建设的客观要求,因而迫切需要变革。一方面,改革现有“树”状结构,实现指挥控制的网络化。为了减少和克服“树”状指挥体制的弊端,应当以“有利于信息的快速流动”为原则改革指挥体制,将以垂直指挥关系为主的树状结构改变为“外形扁平、横向联通、纵横一体”的扁平网状结构。外形扁平是指尽量多的作战单元同处一个信息流动层次;横向联通是指平级单位之间能直接沟通联系,作战平台之间能实时交换信息;纵横一体则是指通过计算机和网络的相互联结使整个指挥体制浑然一体。另一方面,要减少指挥层次,实现指挥控制的扁平化。信息技术的发展,使传统的战场结构、作战方式、时空观念和“集中式”、“逐层式”指挥体制面临着严峻挑战。通过广泛运用电子计算机和提高信息搜集、处理、传输及显示能力,使军队各级指挥机构与控制系统形成互联网络。这将使得指挥体制因减少层次而呈现出横宽纵短的扁平状态,使尽可能多的作战单元同处在一个信息流动层面,实现信息共享。扁平化的最大特点是横宽纵短,纵横一体,既减少了指挥层次,又缩短了信息流程。扁平化、网络化指挥体制由于信息渠道纵横交错、节点多,机动用户可随时在网络中与多个节点沟通联系,具有传输距离远、精度高和抗毁能力强、保密性能好等优点;能将战场上分散配置和单

独作战的兵力兵器连接在一起,最大限度地组合各种作战力量,从而提高军兵种协同作战和远程精确打击能力。

## 4 综合保障信息系统综合集成

综合保障信息系统综合集成是指从信息化战争要求出发,坚持以信息为主导,依托信息化整合保障力量、保障资源,改变原有的逐级自我保障、军兵种分立保障的模式,建立战区、军种两级保障体系,形成新的物流配送方式,实现一体化保障。

### 4.1 建立灵活高效的综合保障指挥机构

高技术局部战争作战力量高度结合的特点,给作战保障带来了保障对象多元、协同单位多向、保障内容复杂的局面,要求作战保障必须实行集中统一的组织指挥,必须建立与军队作战指挥体系和战场实际情况相适应的综合保障指挥机构,为战时实施集中统一指挥和联合保障奠定基础,做到关系顺畅、指挥高效。首先,要建立与作战指挥相结合的综合保障指挥体系。在综合保障指挥机构的设置上,要按照作战指挥的总体要求,组建机构精干、结构合理、指挥层次少、指挥效率高的指挥机构。在指挥关系上,受同级作战机构的统一指挥,并接受上级保障指挥机构的指导。在指挥职能的划分上,以作战需求来引导保障指挥,对保障力量实施统一指挥和组织协调。其次,要建立快速、高效、多能、配套的综合保障补给格局。未来战争的节奏大大加快,战场地域扩大,前后方概念淡化,战争的破坏性和打击强度大幅度增强,装备损坏率大大增加等因素,要求必须建立与之相适应的保障补给格局。这种补给格局应该是上下衔接、纵横相连、多层次、多力一向、多渠道、多手段的保障整体。具体要求包括:一是能有效地进行全力一位保障。即既能纵向保障,又能横向保障,并便于广泛机动地调整保障力量,使部队无论在哪个力一向、哪个地区作战,均可得到保障。二是便于保障力量的统一调整使用,迅速形成新的保障重点。三是有利于冲破敌人的封锁。再次,要加强综合保障指挥自动化系统的建设。综合保障指挥自动化系统是连接各级综合保障指挥机构的神经中枢,是确保综合保障指挥顺畅的重要物质基础。应当按照整体配套、功

能先进、长远规划、分步实施的原则,高起点、高标准地抓好综合保障自动化系统的建设,做到既要保证与本级作战指挥系统全面联网,又要实现保障系统内部的顺畅指挥;既要搞好与上级保障部门的对接,又要延伸到基层保障单位,实现资源共享,形成具有我军特色的分散式、多节点、多通道的综合保障指挥自动化系统。

### 4.2 建立科学的联合作战物流中心

军事物流是一门新兴学科。从伊拉克战争来看,军事物流中心的作用不可低估。战前,美军在科威特、卡塔尔等国开设的大型军事物流中心,与美军在海湾地区的常设军事基地相配合;战中,则极力追求从军工生产车间到前线散兵坑的全程物流精确控制,并实行快速投送。我军综合保障信息系统综合集成应该借鉴世界发达国家的成功经验,改变物资分散存储、分散筹措和临时开设预储基地的做法,集中建设一批大型物流中心,把传统的按专业划分的物流模式转变为按功能划分的物流模式,实行模块化组合,搭建分布合理、运转快捷的物流配送网络。此外,还应该开发应用先进的军事物流技术,打破军兵种界限,充分利用我军物资源,实行物资集中管理和配送,为应付突发事件、实施大规模投送创造条件。

### 4.3 实现精确保障和可视化后勤

实现精确保障和可视化后勤,即利用综合信息系统,在战场上建立起现地与后方基地间的可视联系,指导战场上的各种抢救抢修等保障工作。首先,要借助一体化信息系统使后勤装备部队的行动和物资储备的情况近实时地显示在指挥中心,准确报告物资消耗和装备损耗情况,而作战部队也可随时将作战物资的需求情况、战损车辆和受伤人员的情况以图形、图像的形式显示在后勤装备指挥人员的计算机屏幕上,可以精确指明战损车辆物资的情况和位置,后勤装备部队能够有针对性的进行保障人员和器材准备,不会出现保障不到位或保障器材不配套等情况,使保障更加及时有效。其次,各级指挥机构应具有对作战损耗进行汇总、上报及分析功能,能够根据作战损耗情况生成后勤装备保障通用态势图,在评估后提供最合理的方案,指挥员可以准确计划和实时协调保障力量,并可以利用图文形式发送到保障机构,使作战部队的消耗得到及时

补充,伤员得到及时救治。第三,利用一体化信息系统,可以在战场上建立起现地与后方基地间的可视联系,指导战场上的各种抢救抢修等保障工作。

#### 4.4 多种保障方式综合运用

在信息化战场,后勤保障将以“蛙跳式”和“携行式”为主要方式。其基本结构是:把后勤指挥管理机构和后勤基地主本尽量配置在战略后方,前方只建立小型的后勤指挥所和携带少量急需物资的“携行式”保障分队,减少战场展开的后勤规模,作战部队通过前方后勤指挥所的数字化 C4I 系统与战略后方基地保持密切的联系。战斗中根据需要,后勤系统要依靠空运,以“蛙跳式”的方法,在前

方或敌后方建立临时性保障基地,利用战斗间隙为作战部队和前方小型化保障分队进行快速补给。临时性保障基地可以由某一级后勤单独建立,也可根据情况由战略、战役、战术三级后勤共同建立。实践表明:定点和伴随保障相结合,检查保养和突击抢修相结合,专业修理力量和驾驶员自修相结合,旧件修理和换件修理相结合,部队保障和地方保障相结合,逐级保障、伴随保障、定点保障、巡回保障和多群、多路、多点保障的有机穿插,有效地形成了各级的独立保障和整体保障网络体系,是高技术作战条件下技术保障反应迅速、抢修及时、抢修能力大大提高的法宝。

#### 参考文献(略)

#### 作者联系方式

通信地址:合肥电子工程学院博士生队

邮政编码:230037

联系电话:0551-5767514 13966753528

# 军队指挥信息系统系统集成模式的探讨

李鸿林 杨涛

**摘要：**信息化建设取得了阶段性的成果，但由于各系统独立开发，没有全局筹划和统一的标准，系统间不能互连、互通、互操作，成为共用能力很差的“烟囱式”系统。系统集成是有效的解决途径，本文探讨了系统集成内涵、模型、措施。

**关键词：**指挥信息系统（C4KISR）；系统集成；模型

为完成机械化和信息化建设的双重任务，实现我军现代化的跨越式发展，全军部队展开了作战任务为牵引的重难点问题研究，军队信息化建设取得了阶段性的成果。随着我军的信息化的发展，军队指挥信息系统的建设也初具规模，但是在发展过程中也存在着由于各系统独立开发不成体系，不能有机结合，无法发挥整体作战效能的问题。为了巩固信息化建设成果，进一步推进信息化进程，必须继续以指挥信息系统建设为突破口，抓好系统集成，全面整合指挥信息系统和其他信息建设成果。本文就军队指挥信息系统的系统集成问题展开探讨，提出综合集成的模式和可行的技术路线。

## 1 系统集成是发展的必然

在海湾战争中，美军的 C4I 系统，由于各自独立、封闭式的综合技术使得系统间失去了互通、互操作的能力，C4I 系统成为“自动化孤岛”，成了共用能力很差的“烟囱式”系统。海湾战争后美国国防部通过深刻反思，决定放弃原来的孤立式的开发和管理方针，改为采用开放式系统工程方法，最终形成了 C4KISR 战略，系统集成是其关键技术。美军的系统转型对我军的指挥信息系统建设是一个很好的启发。指挥信息系统作为综合军事信息系统，其发展过程是一个信息技术不断集成的过程，由早期的指挥控制，扩展到情报侦察、预警探测、通信、电子对抗、辅助决策、火力打击控制等领域，其应用已覆盖了作战的全过程。目前的作战指挥、作战保障、战役战术训练、办公自动化、财务工作、装备管理、通信维修等应用系统，研发的渠道、背景、时间和具体的标准、协议、规范及基础

平台不同，导致了系统相互不兼容，只有实现对各系统的全面系统集成，形成一体化的指挥信息系统，我军作战指挥效能才能高效发挥。

## 2 系统集成内涵

指挥信息系统本身不是一门科学或技术，是集指挥、控制、通信、情报等功能于一体的系统工程，涉及多种学科和技术。指挥信息系统的系统集成必须以网络为支撑，以数据为核心，实现系统功能和数据的互联、互通和互操作。

### 2.1 定义

系统集成就是根据作战指挥、部队管理、教育培训、政治工作、后方勤务、装备管理、日常办公的需要对多种系统和技术进行剪裁，恰当合理地选择相关技术和策略，使系统地整体性能上达到最优化、技术上具有先进性、实现上具有可行性、使用上具有灵活性和可扩展性。

### 2.2 组成要素

指挥信息系统是具有特定功能、适用于特定复杂信息的系统，是由从上至下各级指挥所的物理和逻辑的连接构成的有机整体。战区指挥信息系统包括：战区本级指挥所、战区主要业务处理中心集团军（省军区）、师（军分区、警备区）指挥所系统、团指挥所以及主要业务保障系统（中心）等。每一级的指挥信息系统由若干要素构成，每一个要素又由硬、软平台、支持软件、共性应用软件（技术子系统）和专用应用软件等构成。系统集成的组成要素主要包括系统体系结构、网络拓扑结构、硬



件设备、软件系统等。

### 3 系统集成模型

指挥信息系统的集成模式包括硬、软平台集成、技术子系统集成、要素集成、物理节点（分系统）集成、大系统集成等，如图1所示。其中总体设计和系统集成主要包括需求调研、规划设计、系统总体解决方案等，并包括组织、协调物理分系统与技术子系统的集成联试等；各技术子系统负责完成各要素的公用复用软件。在具体实施时可以从以下五个方面加以考虑。

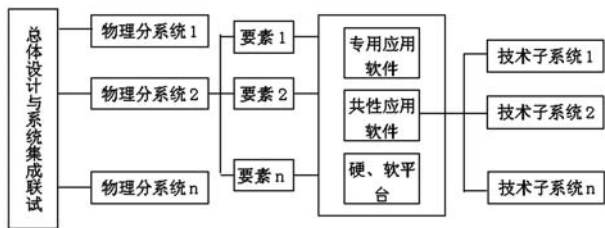


图1 指挥信息系统的集成模式

#### 3.1 硬、软件平台

指挥信息系统硬、软平台的集成就是指将不同的硬件平台、软件平台、开发工具以及有关系统支持软件等集成为一个统一高度协调运行的应用平台，用户可共享系统硬、软资源。硬、软平台是指指挥信息系统工程建设的基础，其性能优劣直接影响系统的性能，在选型和集成过程中，应综合考虑总体要求、体系结构、软件平台和硬件平台等。

##### 3.1.1 总体要求

硬、软平台的选型既要遵循一般信息系统平台的选型规律，走开放式国际标准化道路，又要满足部队指挥控制的实际作战需求和应用开发要求，即要与全军指挥信息系统互联互通，并符合五“统一”（统一通信接口、统一编程接口、统一用户接口、统一系统管理与服务管理、统一信息格式和数据格式）要求，以及满足一定的抗干扰和信息安全保密要求。

##### 3.1.2 体系结构

体系结构的选型是系统集成的首要环节。它是针对部队真正需求，选择合适的计算技术，确定合

适的体系结构，如集中式系统结构或分布式结构，同时确定相应的网络拓扑结构，即整个系统可以划分的局域网数，每个局网的类型，局网与局网之间的连接方式，采用的网间协议等。

##### 3.1.3 软件平台

软件平台的选型就是选择合适的操作系统、网络操作系统、数据库管理系统以及程序设计语言等。其中操作系统的选择应考虑实时多任务、互通性和安全性，网络操作系统的选择应考虑综合、实时、可靠传输的要求。在考虑操作系统的性能的同时还要考虑它的易用程度、网络软件、DBMS，编程语言、CASE，各种支持软件能否满足需求等多种因素，要慎重地在先进性和成熟性方面予以权衡。因此建立软件平台时，要作周到的考虑，保证各项功能需求都经过实验验证，且集成后能正常运行。

##### 3.1.4 硬件平台

硬件平台主要包括PC机、工作站、服务器、网络设备、各种I/O设备等在选择硬件时要严格按照全军指挥信息系统建设的设备选型原则进行。

**网络结构** 是系统设计的中心环节，目前的结构常用的是树形和星形结合起来的典型结构，它具有结构简单、可靠性高、系统稳定性好等特点。利用交换式网络技术组网解决通信阻塞问题。

**网络操作系统** 应能满足计算机网络系统的功能和性能要求，一般要做到网络维护简单，具有高级容错功能，容易扩充，可靠性高，具有广泛的产品支持。

**网络服务器** 应考虑速度、容量和可靠性三方面因素。速度和容量比较直观，可靠性方面的内容较多，包括自动恢复、多级容错、环境监视等。

**网络工作站** 网络工作站可以选用名牌机、品牌机和兼容机，一般应考虑长远发展而又实用经济。

**综合布线** 需要考虑的因素很多，如高架还是地沟，楼内如何屏蔽，如何远离动力线，楼外接地等。

#### 3.2 技术子系统及接口设计

将各要素的共性应用软件按照功能要求进行分工，定义有关接口以确保系统间的协调工作。

3.2.1 技术子系统的划分

技术子系统及共性应用软件一般可以按照功能要求进行划分如下：

- 信息（文、图）处理系统；
- 数字地图与地理信息系统；
- 态势显示处理系统；
- 作战综合数据库分系统；
- 作战环境分析系统；
- 系统监控系统；
- 安全保密系统。

3.2.2 接口设计

接口是两个不同系统（子系统）之间的交接部分，包括内部和外部接口。不解决好接口问题，指挥信息系统中各种不同的分系统之间便不能很好地衔接。

**内部接口** 指指挥信息系统内各技术分系统之间的信息传递和调用关系，如文电处理系统与数据

库系统之间、文电处理与图形处理之间、图形处理与应用软件之间、数据库系统与应用软件之间的接口等。

**外部接口** 含义非常广泛，包括指挥信息系统与上级及下级指挥信息系统的连接，同级系统内不同功能系统之间的连接；与各层次的软件、硬件接口及网络通信接口的连接等。

3.2.3 技术子系统和专用软件研制

各技术子系统和各要素专用的应用软件并行地按照需求，依据统一的标准，按通用化，标准化的要求，进行开发。

3.3 要素集成

在各技术子系统和专用应用软件研制完成之后，就可开始进行要素的集成，要素集成的基本内容如表 1 所示，其中专用应用软件根据各要素的需求选配相应的软件。

表 1 要素集成内容

专用软件	指挥控制 情报处理 业务处理	战备、作战业务、辅助决策 情报分析、综合
共性应用软件	文电处理系统 图形处理系统 数据库应用 安全保密 系统监控	文电编辑、收发与管理 地图态势图制作、显示、传输 数据库的使用、维护与管理
支持软件	文字编辑处理 文电处理 图形处理 地理信息系统 工具软件	通用字处理软件，如 Word、WPS、GWS X400、X500 CGM、XGL、XIL GIS、ARC 软件开发，测试与管理等工具软件
硬、软平台	网络软件（协议）	TCP/IP，NFS
	系统软件	操作系统 程序设计语言 数据库管理系统
	硬件	微机、工作站、服务器、网络及接口设备

3.4 物理分系统集成和联试

系统集成技术般可以分为两个层次。第一层次的集成是物理分系统（或全系统）的场外集成联试，第二个层次的集成是在第一层次集成的基础上，即物理分系统（或全系统）的现场集成联试。场外集成联试是在总体技术的指导下，进行系统

软、硬件设备的连接和试验，力求暴露和解决软、硬件存在的问题，检查软、硬件的可靠性，系统中各种接口关系的正确性以及系统中各种人机接口及工作方式的适用性等，在此基础上达到信息集成和部分功能集成的目的。外场集成联试经考核后，系统才能转入现场集成联试阶段。现场集成联试包括各物理分系统在现场的安装、恢复、调试，以及全

系统集成联试。重点在于解决系统之间的互连、互通；解决单个指挥所和单个系统合成指挥功能及工作方式的适用性以及系统的可靠性等。

### 3.5 系统试运行、使用与维护

系统试运行是实现现有系统向新系统转轨的重要一步。它一方面使新系统在实际环境中进一步验证各项功能和性能指标，在使用中边用边改，逐步完善；另一方面使具体使用人员逐步适应新系统，并不断充实历史数据等。系统经试运行证实其功能和性能均满足设计要求时，便可组织对新系统的鉴定验收。

## 4 抓好系统集成的措施

### 4.1 提高指挥信息系统建设在信息化建设中的地位

提高指挥信息系统建设在信息化建设中的地位，一方面调整和提高组织管理机构的层次，另一方面提高指挥信息系统有关项目的优先等级。针对具有全局影响力的“瓶颈”难题，提高其研究的优先等级，在部队的作战能力向信息化迈进的建设过程中，可以起到牵一发而动全身的积极带动作用。

### 4.2 制定纲领性的发展规划

强调系统集成的指导思想，突出全局筹划。在系统建设的过程中，不断总结经验，逐步提高认识、更新观念，围绕加强系统集成这个中心，突出顶层设计和综合建设，制定出纲领性的发展规划，在侧重于局部发展的同时，贯彻以全局统率局部的发展思路。

### 参考文献（略）

### 作者联系方式

通信地址：云南昆明 77200 部队自动化工作站

邮政编码：650032

联系电话：13888090489

### 4.3 注重软环境建设

软环境包括指挥信息系统制定的各种方针政策、标准原则、体系结构框架、管理方法以及有关的规章制度等。指挥信息系统的建设，是为了实现战区各兵种系统互连和作战指挥信息资源共享，形成综合统一的指挥与控制。因此，必须在统一标准规范、统一技术体制上下功夫，尽快实现系统的标准化。

### 4.4 以新的作战理论指导系统发展

新技术的研究开发及其在军事领域的广泛应用，不断促进军事领域的变革和发展，推动着军队武器装备、体制编制和军事理论的发展进步。而军队建设水平的提升，尤其是军事理论的创新和实践，会不断提出新的军事需求，这就需要我们不断地推动指挥信息系统在概念和功能上的拓展以及在可靠性、安全性和生存性等方面的不断增强和完善。

## 5 结束语

作战部队作为指挥信息系统的直接使用者，应着眼于未来信息作战的特点及对指挥信息系统的要求，结合部队对指挥信息系统组织运用的实践及经验，指挥和技术人员对系统的改进意见等，进行综合论证，提出系统综合集成的需求。依靠部队自身的技术力量，合理借助军地科研院所的技术力量，围绕一体化指挥信息系统的建设，强化信息化建设阶段性成果的综合集成，持续提高信息化建设的整体效益和部队整体信息作战能力。

# 网格环境下分布式异构数据库的数据集成 ——建立资源描述的本体模型

李君灵 杨晓超 蒋维

**摘 要:** 从本体的技术角度出发, 本文描述了异构数据库数据集成中不同层次的本体的建立, 较好地解决了异构系统中数据类型、数据结构、数据格式等方面的差异, 实现了异构系统的无缝连接, 为最终解决训练领域中异构数据库数据集成问题打下了坚实的基础。

**关键词:** 本体; 领域本体; 分布式异构数据库; 数据集成

## 1 引言

目前, 许多指挥训练模拟系统的数据来源于分布式异构数据库。在这样数据库中, 由于数据资源分散, 类型繁多以及不同节点数据结构的不一致, 而且缺乏统一的规范和标准, 使得不同的数据结构的制定者对于相同的实制数样出现了语义上的差异, 造成数据管理上的困难, 从而使得系统间的数据资源的共享不能够很好地实施。因此, 要真正实现资源的共享和决策支持, 必须消除异构数据库中数据的冲突、异常, 对网格环境下分布式异构数据库进行数据集成。

而消除异构数据库中数据的冲突、异常的有效方法之一就是引入本体。本体 (Ontology) 关注的是客观现实的抽象本质, 起源于哲学。它包含 4 层含义: 概念模型、明确、形式化和共享<sup>[1]</sup>。利用本体, 可以捕获军事训练领域的知识, 确定该领域内共同认可的术语 (概念), 提供人和机器对该领域知识的共同理解, 并给出这些概念之间相互关系的明确定义, 即可以从语义和知识层次上描述信息系统的概念模型, 从而很好地解决数据在语义上的冲突问题, 提高数据的共享程度和数据处理的准确度。

因此, 本文从本体的角度出发, 建立了不同层次的本体, 定义了异构系统间数据定义和交互的规范, 使数据共享成为可能, 很好地实现了异构系统资源的表示、组织和交互。

## 2 异构数据库的数据集成

### 2.1 异构数据库数据集成典型体系结构

异构数据库数据集成典型体系结构为全局概念视图和联邦数据库系统模式<sup>[3]</sup>。

#### 2.1.1 全局概念视图模式

该模式是早期的数据库集成。该模式下, 各局部数据库间耦合紧密, 各局部视图统一集成为一个全局视图。该体系结构仅适用局部数据库模式不经常变动的静态集成, 且效率较高, 不适用于局部模式经常变动的情形。

#### 2.1.2 联邦数据库系统模式

该模式类似于全局概念视图模式。主要区别是仅需要对局部模式部分集成, 当局部模式变化时, 联邦数据库中的模式可以不变, 这在一定程度上解决了全局概念视图方式中全局模式维护困难的问题。但该体系结构仍需要维护局部模式与联邦数据库模式的对应关系, 系统的开销仍相对较大。

### 2.2 网格环境下基于本体的异构数据库数据集成体系

针对上述两种典型集成体系, 本文提出了一种综合两者优点的集成体系——网格环境下基于本体的异构数据库数据集成体系, 如图 1 所示。

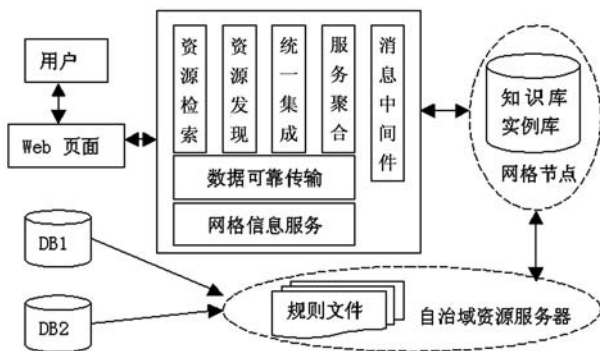


图1 网络环境下基于本体的异构数据库集成体系

其中, 网络技术是分布式计算研究领域的最新成果。网络实际上是一个集成的计算与资源环境(也叫“计算资源池”), 网络是高性能计算机、数据源、因特网等几种技术的有机组合和发展, 它与当前的因特网相比, 具有高性能、一体化、资源共享、协同工作、知识生产等技术优点<sup>[4]</sup>。网络环境的搭建使得各节点的资源发现和优化成为可能<sup>[5]</sup>。

基于本体的知识库和实例库是该集成体系下的全局视图, 它是对军事训练领域资源的总体的统一描述<sup>[6]</sup>。而各个资源子站点可以使用自己独立的本体描述方案来描述自己的资源信息, 在主站点上使用与领域本体一致的公共描述方案, 通过本地文件与公共文件的相互映射来解决异构资源站点间的信息交互, 从而进行分布式的资源检索。这种异构数据的共享和集成模式使得各节点自己维护自己的局部模式, 不会给主服务器造成太大的负担, 而且各个节点可以动态的增加、删除和修改。同时本体的引入使得语义信息得到保留。

网络环境下基于本体的异构数据库集成体系把描述整体资源的全局视图(知识库)存放在网络节点中, 同时资源提供者把自己节点与统一视图之间的映射规则文件存放到自己指定的自治域资源服务器上, 分布存储于自治域资源服务器中的映射文件受各个资源管理安全域及共享策略的约束, 并与网络安全设施相绑定, 以建立信任关系约束。网络节点中的元数据提供包含资源内容、上下文情境、关联、位置等的资源描述, 为能够高效地发现、选择、查找、组合及重用资源奠定了基础。

基于本体的异构数据库数据集成过程如下。

1) 建立本体模型: 根据各个数据源的结构、特点抽取信息, 形成全局的概念模式(自上而下), 建立起应用的本体模型, 包括分类系统和共享属性集;

2) 描述数据实例: 根据模型描述每个数据的元数据信息, 将它们转换为描述实例文档;

3) 查询转换: 利用分类系统和推理机制进行查询;

4) 检索结果呈现: 以用户能理解的方式呈现给用户。

本文将重点介绍基于本体的异构数据库数据集成的第一步——本体模型的建立

### 3 基于本体的全局视图的建立

异构数据库数据集成的关键一步在于建立统一的全局视图, 即建立相应的本体。将本体划分为多个层次可以较好地实现共享和重用。本文将本体划分为顶层本体、领域类本体和应用本体, 如图2所示。

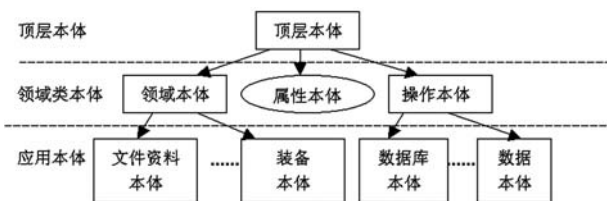


图2 本体的层次划分示意图

应用本体相对易于理解, 下面重点介绍顶层本体和领域类本体。

#### 3.1 顶层本体

顶层本体描述的是最普遍的概念以及概念之间的关系, 如空间、时间、事件、行为等等, 它独立于具体的应用领域。

3.2 领域类本体

领域类本体可以细分为领域本体、属性本体和操作本体。

3.2.1 领域本体

该本体描述某领域内部术语和概念的集合，以及该领域内通用的信息词汇表，包括域内基本概念和相互关系的描述。平台需要建立的领域本体包括训练领域数据元语概念、它们的定义、它们之间的关系以及该领域的术语和公理。这个本体包括 13 个抽象的本体概念基本类，然后大约有数百个的子类从基本类继承，比如：水文环境、气象实况等。

领域本体的建立用来消除语义方面的差异，通过刻画概念之间的关联实现一定领域内专用词汇意义的共享和交流。

领域本体是关于训练领域中对资源框架的描述。这部分的建立主要由专家给出训练领域中的框架。本文以训练领域中的文件资料为例，建立了如图 3 所示的描述框架。

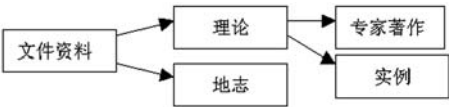


图 3 领域本体的描述框架

3.2.2 属性本体

属性本体中定义的属性都是从各领域本体中抽取的公共属性。属性的定义必须是规范且有权威的。属性的建立主要通过专家和知识工程师的交互完成。属性的确定主要由专家和知识工程师参照相关规定。关键词提取的方法参考文本分类过程中关键词库的建立方法，选用了最简单的互信息量的方法： $w = c_i / C$ ，其中  $c_i$  表示单词在第  $i$  中出现的次数， $C$  示在所有类中出现的次数。选定一个阈值  $W$ ，然后将  $w$  与  $W$  进行比较进行选定。

本文以文件资料为例对其公用属性进行了标准化的抽取，简单示意图如 4。

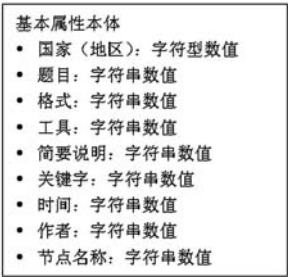


图 4 属性本体示意图

3.2.3 操作本体

操作本体和具体的数据信息已经无关。它是在异构数据共享的情况下如各节点对自己的定位和操作方式等描述。它的建立主要是用来消除异构系统间两个层面上可能存在的差异，如系统级的异构（指不同的主机、操作系统和网络）和结构级的异构（指数据结构、接口和模式上的不同）。

操作本体的定义比领域本体和属性本体都要复杂。领域本体和属性本体都没有本体之间的调用。但是在操作本体中有本体间的相互调用。

操作本体中数据对象实体是最通用的定义，简单定义如图 5。

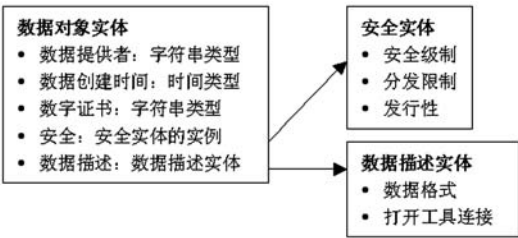


图 5 操作本体的定义示意图

4 基于本体的全局视图的编码实现

基于本体的全局视图的编码实现主要包括建立各种不同层次的本体及其实例和关系。

4.1 本体、实例和关系的建立

4.1.1 本体的建立

本小节简单介绍领域类本体的建立。

(1) 领域本体

从图 2 可以看到在以文件资料为例的情况下领域本体就是以文件资料为根。该根下都是以类的形式编入本体，构成一颗领域树。

(2) 属性本体

以一个大类的形式出现，其中具体的属性以概念的属性形式出现。

(3) 操作本体

操作本体的定义比较复杂，它既包括类的形式，也包括本体的形式。

4.1.2 实例的建立

有关需要定义的实例都是操作本体的实例。分别定义如下：

- 数据库实体的实例：基本的关系型数据库，如 mysql、oracle 等
- 数据描述实体的实例：如数据是 PDF 格式，相应的打开工具是 Adobe Reader，同时提供链接地址

#### 4.1.3 关系的建立

本体是以关系为中心的，本体强大的知识表达能力与知识推理能力都是以关系为基础的，所以关系的建立是本体编辑的核心。该部分主要分成两部分完成：关系定义和关系实例定义。

#### 4.2 本体简单示例

本体的实现工具主要采用的是斯坦福大学开发的 protege3.2，protege 是基于 java 开发的开源工具，能够支持插件的开发，提供了较好的本体开发环境，并且支持中文的输入法。在实现阶段，我们采用 OWL 来描述本体模型。OWL 作为 W3C 的推荐标准，是其所倡导的语义万维网（Semantic Web）的核心技术之一，意在提供一种语言，能够用于描述 Web 文档和应用中固有的类和类之间的关系。它通过定义类和类的属性来形式化一个领域，声明、定义对象和对象的属性，以及在 OWL

形式化语义允许程度上对类和对象进行推理。因此这种具有语义化特点的简单数据模型和语义描述，可以较好地满足语义化本体建模和知识表述的需求。部分 OWL 文档如下所示：

```
<owl: ObjectProperty  ResourceType>
<owl: domain rdf:about =ResourceDescription>
.....
</owl:ObjectProperty>
```

该文档说明在资源本体中有对象属性 ResourceType，它的值域必须是 Resource Description 类的实例。

### 5 结束语

为了适应未来信息化发展的需要，能够在训练领域实现数据资源的共享的系统是非常必要的。而在实现资源共享的过程中，通过本体来描述分布式资源，才不会造成语义的丢失，从而实现各单位之间系统无缝连接。通过对本体的全面描述，可以使各个不同的节点的资源文件实现映射关系，从而使得异构系统中的信息能够实现交互。另外通过本体可以对资源实现基于语义的检索。

#### 参考文献

- [1] Karp, V., Chaudhri, S. and Thomere, J. XOL: An XML-based Ontology Exchange Language[R]. Technical Report, Department of Computer Science, University of Maryland, 1999.
- [2] 鲁鸣. 基于本体的异构导航数据库集成与空间信息语义服务研究[D]. 上海, 华东师范大学, 2006.
- [3] 强保华. 异构数据库语义集成技术研究[D]. 重庆, 重庆大学, 2005.
- [4] 陈磊, 韩颖, 李三立. 信息网格中基于本体的 Web 服务动态集成和重构[J]. 软件学报. 2006, 17 (11): 2255-2263.
- [5] 陈小武, 潘章晟, 赵沁平. 网格环境中模式复用的异构数据库访问和集成方法[J]. 软件学报. 2006, 17 (11): 2224-2233.
- [6] Heflind, H. and Shoe, S J. A Knowledge Representation Language for Internet Applications[R]. Technical Report, CS-TR-4078 (UMIACS TR99-71), Department of Computer Science, University of Maryland, 1999.

#### 作者联系方式

通信地址：南京市 1406 信箱三部

邮政编码：210007

联系电话：13584011479 025-84288300

# 电子对抗软件工程标准体系的研究与建立

李强 钟晓峰

**摘 要:** 本文在对我军军用软件工程标准做一简要回顾后,探讨了电子对抗软件工程标准问题,提出了电子对抗软件工程标准体系并建立电子对抗软件工程标准体系框架。

**关键词:** 软件工程; 标准; 电子对抗

## 1 引言

软件是军用电子信息系统、电子对抗系统的重要组成部分,随着装备信息化的发展,软件在军用电子信息系统、电子对抗系统所占的比重也越来越大,软件的质量对发挥军用电子信息系统、电子对抗系统的作战能力的影响也就越来越大。过去,装备功能的 80%是由硬件实现的,软件只完成 20%的功能,今天,随着装备信息化的发展,装备功能的硬件和软件的实现恰好做了一个颠倒,即硬件只完成 20%装备功能,而 80%则是由软件完成的。但随之而来的是软件问题占系统问题的比例也大幅度攀升。据统计,系统中软件问题已从占问题总数的 20%上升到 80%,而硬件问题则明显从 64%减少到 14%<sup>[1]</sup>,这反映出军用电子信息系统、电子对抗系统硬件设计、研发、生产水平特别是可靠性水平已经有了大幅度的提高,而软件因其日趋复杂和广泛应用,其质量已成为制约整个系统质量的瓶颈,也即“软件危机”不但没有减轻,反而越来越加剧。软件存在的质量问题,已引起方方面面的高度重视,并相应开展了一些工作、采取一些有力的措施。加强军事需求和作战需求的研究力度、建立一套行之有效的顶层设计的框架和技术、增强软件系统的测试和验证环节等,都是改善、完善并提高软件系统质量的有效手段和方法。但无论是提高软件系统质量与可靠性,还是通过相关的技术措施提高软件系统质量与可靠性,均离不开标准及标准体系的建立和使用。例如,军用电子信息系统是一种集软硬件为一体的、复杂的人机交互式系统。成功建设好一个军用电子信息系统,需要军事人员和技术人员在需求和系统的概念上取得共识。而对于同一个术语和概念的理解,军事人员和技术人员可能会存在很大的偏差。在军用电子信息系统分析、设计和使用

过程中,要想建立军事人员和技术人员对同一个术语、概念和操作的相同理解,就应该为双方建立一套相互可以共识的标准,规范双方对同一个术语、概念和操作的相同理解。因此,标准在军用电子信息系统、电子对抗系统的建设中是极为重要的,标准是军事人员和技术人员相互沟通、交流的纽带或桥梁。本文提出了电子对抗软件工程标准体系和电子对抗软件工程标准体系框架。

## 2 军用软件工程标准建设的简要回顾

军用软件工程标准的建设是随着军用软件、军用电子信息系统的发展而发展起来的,军用软件工程标准化是军用软件、军用电子信息系统建设的重要基础。

### 2.1 军用软件工程标准的发展过程

我军军用软件工程标准的建设大致经历了引进、吸收和使用的三个阶段,军用软件工程标准建设具有引进学习、消化吸收和研究使用的特点。

#### 2.1.1 引进学习

这一时期,军用软件工程标准建设主要是以引进为主,对引进国外先进的软件工程标准进行翻译和整理,在此基础上形成我军的软件工程标准并颁布实施,具有代表意义的军用软件工程标准有: GJB 437-1988《军用软件开发规范》、GJB 438-1988《军用软件文档编制规范》、GJB 439-1988《军用软件质量保证规范》、GJB 1091-1991《军用软件需求分析》、GJB 1267-1991《军用软件维护》、GJB 1268-1991《军用软件验收》、GJB 1375-1992《军用数据库远程访问》、GJB 1382A-1998《军用数据库语言 SQL》、GJB 1419-1992《军用计



计算机软件摘要》、GJB 1566-1992《军用计算机软部件文档编制格式和内容》、GJB 2041-1994《军用软件接口设计要求》、GJB 2115-1994《军用软件项目管理规程》、GJB 2255-1994《军用软件产品》、GJB 2434-1995《军用软件测试与评估通用要求》、GJB 2694-1996《军用软件支持环境》、GJB 2786-1996《武器系统软件开发》、GJB 3181-1996《军用软件支持环境选用要求》等；还有一些指导性技术文件，如：GJB/Z 102-1997《软件可靠性和安全性设计准则》、GJB/Z 109-1998《军用数据库管理系统功能规格说明指南》、GJB/Z 117-1999《军用软件验证和确认计划指南》、GJBz 20111-1993《关系数据库管理系统功能通用要求》等。

这一阶段军用软件工程的标准特点是，以引进为主，大部分标准是参照 ISO/IEC、IEEE 或 DoD STD 相对应的标准编制的，在编制处理上或是等同采用或是一致性程度为非等效。

### 2.1.2 消化吸收

经过一段时间的学习并在一定的范围内的试用或使用上述军用软件的相关标准，发现了其中存在的问题和不能完全适应我军军用软件工程的需要，开始着手修订相关的软件标准，主要涉及：GJB 437-1988《军用软件开发规范》、GJB 438-1988《军用软件文档编制规范》、GJB 1268-1991《军用软件验收》、GJB 2434-1995《军用软件测试与评估通用要求》、GJB/Z 117-1999《军用软件验证和确认计划指南》等，将这些标准分别修订为：GJB 2786-1996《武器系统软件开发》、GJB 438A-1997《武器系统软件开发文档》、GJB 1268A-2004《军用软件验收要求》、GJB 2434A-2004《军用软件产品评价》、GJB 4354-2002《关系数据库管理系统功能通用要求》、GJB 5234-2004《军用软件验证和确认》。

这一阶段军用软件工程的标准特点是，在消化、吸收的基础上，对引进的 ISO/IEC、IEEE 或 DoD STD 的标准认真研究，融合、整理、归并，形成适宜我军使用的军用软件工程的标准。如，GJB 2434-1995《军用软件测试与评估通用要求》主要是参照 ISO/IEC 9126-1991 这个单一的标准制定的，而 GJB 2434A-2004《军用软件产品评价》主要参照 ISO/IEC 14598 系列标准制定。GJB 2434A-2004《军用软件产品评价》将 GJB 2434-1995《军用软件测试与评估通用要求》中给出了软

件质量框架、软件质量特性以及软件的评测过程模型等内容移到了 GJB 5236-2004《军用软件质量度量》中，相对于 GJB 2434-1995《军用软件测试与评估通用要求》来讲，GJB 2434A-2004《军用软件产品评价》的内容安排更加合理，操作性更强。

### 2.1.3 研究使用

这一时期呈现了以下三个方面的特点。

1) 根据国家军用标准的规定，细化本部门对软件的要求，制定适合于本专业领域使用的软件工程的下层标准。如 GJB 4279-2001《指挥自动化系统应用软件通用要求》、GJB 3982《电子对抗装备软件通用要求》（包括：GJB 3982.1-2000《电子对抗装备软件开发要求》、GJB 3982.2-2001《电子对抗装备软件验收要求》、GJB 3982.3-2002《电子对抗装备数据库通用要求》、GJB 3982.4-2001《电子对抗专用计算机支撑平台软硬件要求》、GJB 3982.5-2002《电子对抗装备软件维护要求》），等。

2) 在制定自己专业领域的电子信息系统或指挥自动化系统的相关标准中，对软件提出相应的要求，如：GJB3623-1999《指挥自动化系统质量保证通用要求》、GJB 3747-1999《地地导弹部队指挥自动化系统通用要求》、GJB/Z 1301-2000《指挥自动化系统工程建设渐进获取法指南》等。

3) 制定了软件质量、软件质量模型、软件测试方面的标准，使军用软件工程标准种类更加齐全和齐套。这类标准有：GJB 5000-2003《军用软件能力成熟度模型》、GJB 5234-2004《军用软件验证和确认》、GJB 5235-2004《军用软件配置管理》、GJB 5236-2004《军用软件质量度量》、GJB/Z 141-2004《军用软件测试指南》、GJB/Z 142-2004《军用软件安全性分析指南》，等。这些标准的制定，丰富了军用软件工程标准，使军用软件工程标准的种类更加齐全，基本覆盖了软件工程的生命周期。

## 2.2 军用软件工程标准的分类

军用软件工程的标准种类较多，分类的方法也不尽相同。例如，可以按功能和生存周期对软件工程标准进行分类<sup>[2]</sup>，分成任务功能和软件生存周期。任务功能包括产品工程功能、验证与确认功能、技术管理功能；软件生存周期可分为概念阶段、需求阶段、设计阶段、实现阶段、测试阶段、制造阶段、安装和验收阶段、运行和维护阶段、引

退阶段。但可以按以下的方式进行分类。

1) 按软件开发的过程及其管理进行分类, 可分为: 软件开发类、软件文档类、软件验收类、软件测试类、软件维护类、软件支持环境类、软件质量控制与保证类、软件配置管理类、软件项目管理类等。

开发类标有: GJB2786-1996《武器系统软件开发》、GJB3982.1-2000《电子对抗装备软件开发要求》、GJB1091-1991《军用软件需求分析》、GJB2041-1994《军用软件接口设计要求》; 文档类标准有: GJB438A-1997《武器系统软件开发文档》; 验收类标准有: GJB 1268A-2004《军用软件验收要求》、GJB3982.2-2001《电子对抗装备软件验收要求》; 软件测试类标准有: GJB/Z 141-2004《军用软件测试指南》; 维护类标准有: GJB1267-1991《军用软件维护》、GJB3982.5-2002《电子对抗装备软件维护要求》; 软件支持环境类标准有: GJB2694-1996《军用软件支持环境》; 质量保证类标准有: GJB 439-1988《军用软件质量保证规范》; 配置管理类标准有: GJB 5235-2004《军用软件配置管理》; 项目管理类标准: GJB2115-1994《军用软件项目管理规程》。

2) 按在软件生命周期过程中所起的作用, 可分为: 专业基础标准、软件过程标准、软件质量标准、技术与管理标准、工具与方法标准和数据标准<sup>[2]</sup>。

3) 按标准归口管理和颁布部门的不同, 可以分为: 国家标准、国家军用标准、部门军用标准、工程标准等。国家标准是由国家的官方标准化机构或国家政府授权的有关机构批准、发布, 在全国范围内统一和适用的标准。如: GB/T 19016-2000《质量管理 项目管理质量指南》是国家标准; GJB2786-1996《武器系统软件开发》、GJB3982.1-2000《电子对抗装备软件开发要求》是国家军用标准。部门军用标准由总部机关主管部门编制计划、组织草拟、统一审批、编号发布的软件工程标准, 是在全军各军兵种同一专业领域范围内统一的标准。工程标准是由某一科研型号项目组织制定的且为该项科研型号项目专用的标准。

### 3 电子对抗软件工程标准的建立

电子对抗软件工程标准起步较晚, 于 1995 年

开始酝酿论证电子对抗软件工程标准, 到 1999 年时, 正式立项编制电子对抗软件工程类标准, 大致经历了初始论证阶段、立项编制阶段、建立体系阶段。

1) 初始论证阶段(1986—1996 年), 大致在装备发展的“七五”和“八五”期间。这一阶段电子对抗装备的发展主要是以硬件为主, 几乎没有软件, 即使有一些软件, 软件也是作为硬件的附属产品, 软件还不是装备。电子对抗软件标准几乎是空白, 要使用软件标准, 也是直接采用国家军用标准或引用行业的软件工程标准。

2) 立项编制阶段(1997—2005 年), 大致在装备发展的“九五”和“十五”期间。随着电子对抗装备的不断发展, 软件在电子对抗装备中所占的比例越来越多, 软件不再是硬件的附属产品, 软件是装备, 软件作为电子对抗装备的重要性也越来越被人们所认识。因此, 不仅要发展电子对抗装备软件, 而且为了更好地发挥软件的核心作用, 要建立电子对抗自身的软件工程标准, 特别是软件工程国家军用标准; 不仅要编制在本部门使用的部门标准, 还要编制国家军用标准。1997 年, 总部机关把论证编制电子对抗软件工程国家军用标准的任务下达给了解放军电子工程学院和总参第 54 研究所, 共同完成电子对抗软件工程国家军用标准的论证。经过解放军电子工程学院和总参第 54 研究所的联合论证, 认为电子对抗软件工程国家军用标准应包括电子对抗软件的开发、需求分析、设计、编码、测试、维护、软件质量管理与控制、软件配置管理等标准, 一共 9 项, 于 1998 年上报总部机关。在总部机关的组织协调下, 经过再论证, 认为首批编制的电子对抗软件工程国家军用标准宜为 5 项, 包括的内容是: 软件开发要求、软件验收要求、通用数据库、专用计算机支撑平台软硬件要求、软件维护要求。1998 年上报总装备部并得到批复, 编制电子对抗软件工程国家军用标准, 总名称是:《电子对抗装备软件通用要求》, 共 5 项, 分别是:

第一部分: 电子对抗装备软件开发要求;

第二部分: 电子对抗装备软件验收要求;

第三部分: 电子对抗装备软件通用数据库;

第四部分: 电子对抗专用计算机支撑平台软硬件要求;

第五部分: 电子对抗装备软件维护要求。

编制时间是从1999年开始到2002年历时三年完成。

《电子对抗装备软件通用要求》立项编制,标志着电子对抗软件工程国家军用标准的诞生,从此以后,电子对抗不仅有电子对抗装备论证、研制、设计、生产、管理等国家军用标准,还有了自己的软件类国家军用标准,具有里程碑的意义。

到2000年,《电子对抗装备软件通用要求》第一个标准《电子对抗装备软件开发要求》编制完成,并上报总装备部,得到批准并颁布实施。2002年,随着《电子对抗装备软件维护要求》编制完成,上报总装备部,得到批准并颁布实施。批准的5项国家军用标准是:

GJB 3982.1-2000 电子对抗装备软件开发要求;

GJB 3982.2-2001 电子对抗装备软件验收要求;

GJB 3982.3-2002 电子对抗装备软件通用数据库;

GJB 3982.4-2001 电子对抗专用计算机支撑平台软硬件要求;

GJB 3982.5-2002 电子对抗装备软件维护要求。

这样,历时三年的《电子对抗装备软件通用要求》编制任务顺利完成,标志着电子对抗软件工程国家军用标准已经建立。

2003年又新编制了有关电子对抗装备软件人机界面,数据库种类、内容和格式等国家军用标准,为电子对抗软件工程类标准体系的建立奠定了基础。

3) 建立体系阶段(2006年一),大致是电子对抗装备发展的“十一五”及其以后的阶段。这一阶段是电子对抗装备发展的黄金时期,电子对抗装备的硬件与软件共同、协调和有机地发展。软件是装备、软件出战斗力已成为无可辩驳的事实。因此,电子对抗装备的发展对软件标准不仅有种类的要求,更有质量和内容的要求。同时,一些大型型号项目研制,特别是大型型号软件项目的研制,对电子对抗软件工程标准的要求越来越迫切。这种迫切要求不仅体现在对标准的需求上,更体现在对标准的体系建立上。有了电子对抗软件工程标准体系,不仅能满足电子对抗装备软件发展对软件标准的迫切要求,更能在宏观上加强对电子对抗软件工

程标准建设的指导。因此,在电子对抗软件工程标准的“立项编制阶段”发展的基础上,在“十五”电子对抗型号装备研制取得成果的基础上,在“十一五”电子对抗型号装备研制需求的驱动下,建立电子对抗软件工程类标准体系就成为一项重要的任务了。

综上所述,在总结“九五”、“十五”电子对抗型号装备及电子对抗软件型号装备标准研制、标准化工作的基础上,根据电子对抗装备研制的实际情况,开始研究、探讨建立电子对抗软件工程标准的体系并初步建立了电子对抗软件工程标准体系。从组成上讲,电子对抗软件工程标准应包括:软件开发类、软件文档类、软件验收类、软件测试类、软件维护类、软件支持环境类、软件质量控制与保证类、软件配置管理类、软件项目管理类等标准,如图1所示。

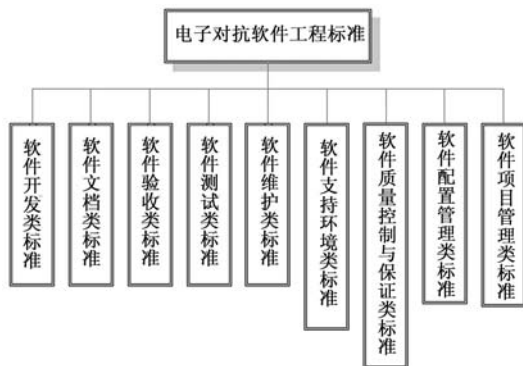


图1 电子对抗软件工程标准组成结构示意图

## 4 电子对抗软件工程标准体系及其建立

电子对抗装备软件工程标准在经历了初始论证、立项编制、建立体系三个阶段和“七五”~“十一五”装备发展特别是“十一五”装备大发展后,建立适应电子对抗装备发展和电子对抗软件工程标准发展需要的电子对抗软件工程标准体系的条件已经成熟。建立电子对抗软件工程标准体系的基本策略是:以国家和军队有关软件的法规、规章、国家军用标准为上层指导文件,形成包括电子对抗软件工程国家军用标准、电子对抗软件工程部门军用标准和电子对抗装备软件型号项目工程标准在内的、相互协调、规定明确、互为补充的电子对抗软件工程标准体系,如图2所示。

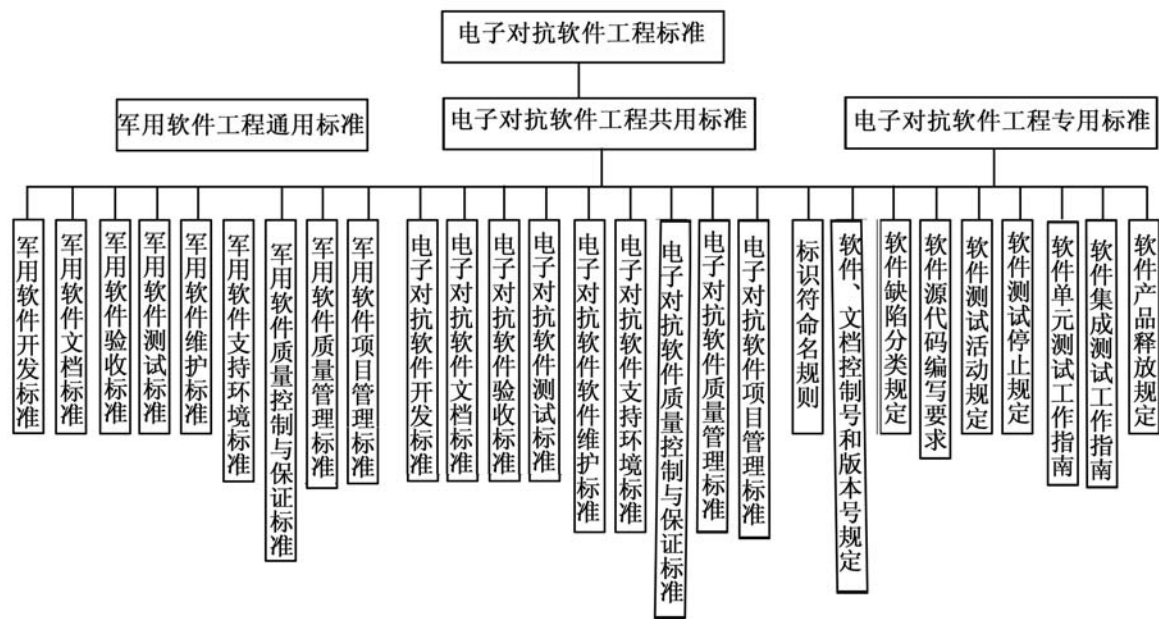


图 2 电子对抗软件工程标准体系组成

图 2 中，军用软件工程通用标准是全军共同使用的标准，因此，通常是以国家军用标准的形式出现的，不仅对一般的军用软件具有指导作用，同时它也是制定电子对抗软件工程共用标准和电子对抗软件工程专用标准的上层标准，是制定电子对抗软件工程共用标准和电子对抗软件工程专用标准时必须遵循的标准，在制定电子对抗软件工程共用标准和电子对抗软件工程专用标准时应保持与军用软件工程通用标准的协调一致。

电子对抗软件工程共用标准是作为军用软件工程通用标准的下层标准使用的，是对军用软件工程通用标准补充，完善因军用软件工程通用标准作为宏观指导性标准而顾及不到的电子对抗软件对软件工程的特殊规定之处，它是全军各军兵种电子对抗领域均要遵守和执行的的标准，所以，这类标准可以国家军用标准的形式出现，也可以部门军用标准的形式出现。

电子对抗软件工程专用标准是适用于具体工程项目的工程标准。尽管已经有了军用软件工程通用标准和电子对抗软件工程专用标准，但对工程项目开发的一些具体规定，在这两类标准中仍不能完全规定，这就需要一定数量的工程标准作为补充，比如，软件源代码编写要求、软件人机交互界面设计要求、标识符命名规则、软件与文档的控制号和版本号等，在不同的工程项目中的规定不一样，这就

需要工程标准作为补充，这也就形成了电子对抗软件工程专用标准。这类标准通常是以工程标准的形式出现的。

4.1 国家和军队相关软件的法规、规章

国家和军队相关软件的法规就是指由国务院、中央军委颁布的有关软件工程的条例，国家和军队相关软件的规章是指总部颁布的有关软件工程的管理办法。国家和军队有关软件的法规、法规，是在总结我国、我军软件工程实践和武器装备软件工作经验基础上制定的，是客观发展规律的具体体现，是确定军用软件工程标准化工作的目标要求、建立军用软件工程标准体系、制定军用软件工程标准工作规划的重要依据。建立电子对抗软件工程标准体系必须严格执行国家和军队相关软件的法规、规章。

4.2 相关软件工程的国家军用标准

相关软件工程的国家军用标准就是指由总装备部颁布实施的有关军用软件工程标准，它是全军范围内均可以使用的软件标准，具有宏观指导作用。如：GJB2786-1996《武器系统软件开发》、GJB438A-1997《武器系统软件开发文档》、GJB1091-1991《军用软件需求分析》、GJB2041-

1994《军用软件接口设计要求》、GJB 1268A-2004《军用软件验收要求》、GJB/Z 141-2004《军用软件测试指南》、GJB1267-1991《军用软件维护》、GJB 5235-2004《军用软件配置管理》等。这些标准是作为制定电子对抗软件工程国家军用标准、部门标准或工程标准的指导文件,是作为上层文件使用的。它覆盖了软件开发、软件文档、软件验收、软件测试、软件维护、软件支持环境、软件质量控制与保证、软件配置管理、软件项目管理等方面的标准,对军用软件提了要求,作了规定。

电子对抗专业领域也可有自己的软件工程国家军用标准。电子对抗软件工程国家军用标准是作为软件工程国家军用标准下层标准制定、使用的,是对国家军用软件工程标准的细化和补充。

### 4.3 电子对抗软件工程部门军用标准

电子对抗软件工程部门军用标准由总部机关主管部门编制计划、组织草拟、统一审批、编号发布的软件工程标准。它是国家军用软件工程标准的下层标准,是结合本部门的特点并对国家军用软件工程标准进行了细化制定的具有本部门特色的标准,是对国家军用软件工程标准补充和完善。应成为全军各军兵种同一专业领域共同遵守的标准。

这一层次的标准宜适于对软件开发、验收、测试、维护、文档要求、软件支持环境、软件质量控制与保证、软件配置管理、软件项目管理等在各专业领域有特殊的要求进行规定,对国家军用标准进行补充。如 GJB2786-1996《武器系统软件开发》、GJB438A-1997《武器系统软件开发文档》是国家军用标准,它对一般军用软件开发、文档做出的一个宏观的规定。电子对抗装备软件在开发、文档的种类和数量都有一些特殊性<sup>[3]</sup>,但在国家军用标准

中未规定,因此,需要编制 GJB3982.1-2000《电子对抗装备软件开发要求》对 GJB2786-1996《武器系统软件开发》、GJB438A-1997《武器系统软件开发文档》进行补充。

### 4.4 电子对抗装备软件型号项目工程标准

工程标准是由某一科研型号项目组织制定的且为该项科研型号项目专用的标准。这类标准是对具体的编码风格、编码要求、标识符、文档编写的格式等做出的具体规定。如:“软件源代码编写要求”、“标识符命名规则”、“软件、文档的控制号和版本号”等,宜于用工程标准的形式加以规范。因为不同的软件型号项目对软件源代码编写、标识符的命名、软件控制号和版本号、文档控制号和版本号等要求均不相同,不能做统一的规定,因项目而异。在软件型号项目中就有《软件源代码编写要求》、《标识符命名规则》、《软件、文档的控制号和版本号》等工程标准。

## 5 结束语

电子对抗软件工程标准体系的建设不仅是电子对抗装备和电子对抗软件工程标准建设发展的需要,而且是我军信息化建设的重要内容,是我军信息化建设的重要基础。电子对抗软件工程标准的建设与电子对抗装备的建设一样,涉及面广、协调难度大,是一项复杂、艰巨但又是意义重大的工作。不仅要抓紧电子对抗软件工程标准及其体系建立的研究,更要加强电子对抗软件工程标准化的研究工作,使其真正能为电子对抗装备的发展起到有力的支持和保障作用。

### 参考文献

- [1] 刘杰生. 军用信息系统软件工程实践—基于 ISO9000 的标准软件过程研究, 一体化联合作战与军事运筹研究. 北京: 国防科技大学出版社, 2005
- [2] 石柱. 软件工程标准手册. 北京: 中国标准出版社, 2004
- [3] 李强, 段继华, 郭震华等. 电子对抗装备软件开发策略的研究. 合肥: 电子工程学院学报, 2003, 22(1)

### 作者联系方式

通信地址: 合肥市黄山路 460 号解放军电子工程学院软件工程中心 邮政编码: 230037 联系电话: 0551-5767439

# 美军C<sup>4</sup>ISR体系结构评估方法研究

李瑛 邹江南 贺梅 张晓蓓

**摘 要:** 本文从美军联合试验和评估计划入手, 重点研究该计划下的“评估 C<sup>4</sup>ISR 体系结构的联合方法(JMACA)”。力图通过研究美军近年来致力于 C<sup>4</sup>ISR 系统体系结构的试验和评估的总体构想、发展策略和具体成果, 为我军体系结构评估提供有益的借鉴。

**关键词:** 联合试验和评估计划; 评估 C<sup>4</sup>ISR 体系结构联合方法

## 1 美军联合试验和评估计划(JT&E)

早在三十多年前, 美军就意识到, 高效的联合作战已经不再是单个军种单独能力的总和。作战指挥员更依靠多军种能力, 这是各军种无法单独完成的。美国防部的联合试验和评估计划起源于 1970 年出台的《蓝带国防小组报告》。报告认为美国缺乏卓有成效的联合作战试验和评估的方法, 在此背景下, 启动了美军联合试验和评估计划(JT&E, Joint Test & Evaluation)。联合试验和评估计划拥有丰富科学的方法, 具备组织灵活和快速反应的能力, 它是美军唯一的专门辅助决策者解决众多联合问题的计划。无论是现在还是未来, 联合试验和评估计划将不断发挥其协调资源, 寻找解决联合问题的有效途径。

2002 年, 联合试验和评估计划进行重组, 由国防部长办公室作战试验和评估主任负责管理联合试验和评估计划, 而在此之前是由负责采办、技术和后勤的副国防部长管理。目的是简化联合试验和评估的决策过程, 使作战人员参与联合试验和评估计划的管理和监督, 执行对作战人员和采购人员均有重要意义的联合作战试验, 提供能够与现有条令和程序快速组合的有用结果。

联合试验和评估计划是在国防部长办公室下属的作战、试验和评估主任的监督下运行的, 其需求来自各战区作战司令部, 通过建模、仿真、试验床和野战演习结合的方法, 帮助作战人员研究解决战术、技术和程序, 改善作战进程和众多 C<sup>4</sup>ISR 系统的体系结构中出现的作战难题。

基本流程是: 先由各作战司令部、国防部各业务局和各军兵种提名; 然后对提名进行评审和筛选, 决定哪些提名可以获得资金并开展可行性研

究; 指定执行联合试验和评估的牵头军种。

确定可行性之后, 就进行联合计划和评估试验。试验分两种类型: 快速反应试验和联合试验。快速反应试验在极短时间内回复作战指挥员迅速出现或正在发展的需求。全过程控制在 6 至 12 个月, 大部分能够在 7 个月内完成。

联合试验是在联合试验和评估计划目的范围内对作战人员的难题进行全面、深刻地评估, 全部过程限定在 3 年之内。

目前, 联合试验和评估计划项目组的试验场所已经增长到包括弗吉尼亚州的亚历山大、萨福克、韩国首尔等在内的 13 处。近两年已完成和正在进行的主要试验有 7 项快速反应试验和 14 项联合试验, 其中包含评估 C<sup>4</sup>ISR 体系结构的联合方法(JMACA)。从这些试验中可以看出美军正加强在一些新的技术领域中的探索。

## 2 评估C<sup>4</sup>ISR体系结构的联合方法(JMACA)

信息优势在未来军事作战中的作用越来越重要, 网络中心战越来越依赖强大和复杂的 C<sup>4</sup>ISR 可互操作体系结构。现今世界局势的动荡使得快速反应、联合作战以及整合繁杂的 C<sup>4</sup>ISR 系统的体系结构成为必须具备的手段。此外, 由于复杂的新系统、软件和程序的不断添加, 在部署每个 C<sup>4</sup>ISR 体系结构之前, 对其进行快速评估和改进将会提高作战人员的信息优势。而美军恰恰认为, “联合特遣部队司令员缺乏有效的方法来快速确定 C<sup>4</sup>ISR 体系结构内的缺陷并提供解决方案”。

于是, 2000 年美军开始进行可行性研究, 2001 年 10 月启动了联合试验和评估计划下的名为

“评估 C<sup>4</sup>ISR 体系结构联合方法 (JMACA)”的研究, 计划于 2006 年 1 月止。由国防部长办公室的作战试验和评估主任管理, 海军牵头, 在弗吉尼亚州萨福克的 Bridgeway 技术中心开展。

评估 C<sup>4</sup>ISR 体系结构联合方法 (JMACA, Joint Methodology to Assess C<sup>4</sup>ISR Architectures) 的任务就是为联合特遣部队的指挥员提供一套工具和程序来迅速地对联合特遣部队提交的 C<sup>4</sup>ISR 体系结构进行部署前的评估, 提高互操作性, 最终支持信息优势的获取。

在理论上, JMACA 研究了体系结构缺陷分类和互操作性故障理论研究。JMACA 把体系结构缺陷分为两种: 与体系结构描述产品相关的缺陷和与体系结构本身相关的缺陷。与体系结构描述产品相关的缺陷可以分为目的、标准一致性和目标表述三方面的缺陷。概念上的整体缺陷则与实际的体系结构相关。它们可以区分为功能范畴或结构范畴的缺陷。功能缺陷与适当的功能分布或行动和信息流方面的问题相关。结构缺陷则与视图的界限或一致性, 包括互操作差距和故障在内的问题相关。

而互操作性故障按寿命周期划分, 分为早期、中期和相对成熟期。在两个系统开始互操作之后的早期阶段, 故障率出现较高, 这主要与两个系统之间缺乏互操作经验相关。之后, 出现故障率较低的中期, 这主要与两个系统之间有了互操作经验相关。第三个阶段是故障率再次提升的退化阶段, 这主要是由于新软件的引进和硬件的升级造成。

JMACA 分五步实现的: 第一步: 数据挖掘——收集系统配置和风险信息; 第二步: 系统/综合的风险评估——广泛的系统/综合视图分析; 第三步: 细致分析——详细的功能/任务分析; 第四步: 端到端测试——物理的硬件/软件实验室测试; 第五步: 作战分析。最后向权威机构联合特别工作组和联合部队司令官提出建议要改进的地方, 最终加以实施。总的来说, 就是明确工具和分析需用的数据; 明确体系结构范围的风险; 有选择地对高风险区域进行分析; 提出体系结构的建议解决方案。

五个步骤是通过一系列的集成工具来实现的。这些工具主要有: 网络赋能的时间进度分析系统, 互操作性风险评估联合工具, 网络中心战分析模拟器、联合互操作测试司令部试验床, 联合 C<sup>4</sup>ISR 集成设施、联合分布式工程化平台等等。

JMACA 从 2001 年 10 月开始试验计划, 先后经过了三次检验试验。第一次在 2003 年 9 月的伊拉克自由行动中, 对时间敏感目标体系结构进行了试验。第二次在 “联合特遣部队 04-2” 的模拟实战大规模演习中。第三次是在 “红旗 05-1” 演习中。

在对 JMACA 进行联合试验的过程中, JMACA 已经与现有国防部体系结构计划开展了集成和协作。目前能确定的用 JMACA 来评估的体系结构有: 时间敏感目标、战斗搜索和救援、近空支援、非战斗撤退行动、特种作战部队作战等等。

JMACA 还为一些国防部体系结构研究计划提供了支持, 改进了各军兵种和联合作战的集成。包括: 海军/海军陆战队的网络作战司令部 N8、大西洋战术训练集团、空间作战、海军海上开放体系结构、海军陆战队作战发展司令部; 空军的空军指控情报监视与侦察司令部、空军电子系统司令部; 陆军的训练与条令司令部、通信司令部、通信电子司令部; 联合的美国联合部队司令部 J8 (联合战斗管理指挥控制)、作战指挥员、联合互操作测试司令部。

JMACA 的重要作用 and 贡献是: 为 C<sup>4</sup>ISR 的集成铺平道路; 为 C<sup>4</sup>ISR 互操作性提供风险论证; 进行快速作战分析; 与联合团体合作, 加快 C<sup>4</sup>ISR 集成和转型计划。

JMACA 从开始计划研究起, 就与各个团体紧密合作, 参与国防部及各军兵种的主要计划中, 充分发挥评估效能, 致力于使空中、水面、陆地、水下 C<sup>4</sup>ISR 作战和系统体系结构可以互操作, 最终达到加快众多 C<sup>4</sup>ISR 体系结构的集成和转型的目的。如: 与国防部合作 GIG; 与海军/海军陆战队合作力量网计划; 与空军合作 C<sup>2</sup> 星座计划; 与陆军合作目标部队计划; 与海岸警卫队合作集成深水系统计划等。

### 3 对我军的启示

通过研究美军在评估这一重要环节上的一些具体做法, 可以概况总结出一些美军的经验做法, 这些做法给我们一些有益的启示, 对我军的体系结构评估具有重要借鉴作用。

### 3.1 联合试验与评估是装备科研、采购、运用极其重要的环节

联合作战和网络化扁平指挥需要一体化信息系统。一体化信息系统是由不同功能领域的众多子系统构造的系统之系统，为增强系统之间的互通性与互操作性，提升整体作战效能，必须进行联合试验与评估。为避免装备科研、投资风险和装备运用风险，必须对综合电子信息系统进行联合试验与评估。因此，我军要高度重视联合试验与评估在综合电子信息系统发展中的战略作用，加强联合试验与评估环境建设，加强联合试验与评估方法的研究，并加强这方面的投资。

### 3.2 建立完善各级评估机构，明确各自职能

美军一向重视战略管理，突出全局筹划。在信息化建设的进程中，不断总结经验，逐步提高认识、更新观念，围绕加强系统集成这个中心，突出顶层设计和综合建设，制定出了纲领性的发展规划。全面系统的评估是美军信息化建设中的重要环节，它能够从选题立项、开发研制、功能实现、作战使用、采办等多个环节对在研项目进行验证和评估，从而保证建设方向的正确合理，人力、物力、财力和信息等资源的高效利用，以满足作战需求，提高作战效能。为此，美军首先建立和完善了各级评估机构和体制，在国防部长办公室、军种部和国防信息系统局下设立了专门评估机构。由这些各司其职的评估机构共同完成美军的各项评估任务。

### 3.3 注重全军联合评估，由国防部长办公室顶层统管

美军从上世纪末开始提出军事转型，军事转型

的本质是建设信息化军队，特别是建设以综合军事信息系统为核心的信息化武器装备体系。要发展全军共用的综合军事信息系统，就必须重视纵横融合，积极推进互联、互通、互操作能力建设。这不仅是个技术问题，而且是实施军事转型的战略举措。前国防部长拉姆斯菲尔德说，“军事转型最关键的可能不是研发某些武器系统，而是系统间的互联、互通、互操作能力的显著增强”。对任何在研武器系统来说，进行各军兵种的联合评估显得尤为重要。为此，美军从三十多年前就开始了庞大的联合试验和评估计划，专门负责实施多军种联合试验评估。并且充分考虑到可能出现的各军种之间的利益冲突和各自为政的偏见，美军将联合试验和评估计划的统管职责由副国防部长移交给国防部长办公室下设的作战与评估主任。统管层次的权威性，能够保证顺利、有效、公正地实施联合试验和评估。

### 3.4 采用科学方法，进行定量评估

现今的网络中心战越来越依赖复杂的  $C^4ISR$  系统，针对这种状况，美军及时地开展了对  $C^4ISR$  体系结构进行联合评估的研究，使用现有的工具和数据库，开发科学的方法论，采取建模、试验和作战演习的方式，提供迅速、及时的评估，力图在系统部署前解决作战人员的难题。与此同时，美军还开始了对体系结构备份计划的开发和评估的研究。这种科学的试验方法不是简单的演示，它实现了根据任务对  $C^4ISR$  体系结构的性能进行定量评估，验证了  $C^4ISR$  体系结构互操作性能的衡量标准，建立了体系结构评估基线。

参考文献（略）

作者联系方式

通信地址：北京丰台大成路 13 号

邮政编码：100039

联系电话：010-66820343



# 分布式网络化作战及其建模

刘宁宁 单维峰 朱巍

**摘 要：**分布式网络化作战理论已经被美国国防部和各军兵种普遍接受，并已成为军事变革的核心思想和军队转型的重要基石。本文在分析了分布式网络化作战理论的背景的基础之上，建立了一个分布式网络化作战模型，并以美军数字化营为例，对该模型作战效能进行了分析和评估。

**关键词：**分布式；效能；建模

## 1 分布式网络化作战理论的背景

所谓“分布式网络化作战”就是以“分布式兵力”和“网络化控制”为两个基本要素的面向信息化战场的全新作战样式。“分布式网络化作战”是通过将各作战单元网络化，利用通信系统和计算机系统组成的信息栅格网，将分布在陆、海、空、天的各类情报侦查、预警探测、指挥控制、通信、电子对抗系统和武器平台有机结合，形成统一高效的作战体系，实现战场态势高度共享、部队协调自我同步、作战行动实时并行，发挥出最大的整体作战效能。美军认为：当前一体化联合作战还只是“网络中心战（NCW）”的初级阶段，而“分布式网络化作战”（Distributed Networked Operations）才是“网络中心战”的发展目标，分布式网络化的作战理论已经被美国国防部和各军兵种普遍接受，并逐渐成为军事变革的核心思想和军队转型的重要基石。

## 2 分布式网络化作战模型

根据分布式网络化作战的思想，本文建立了一个新的分布式网络化作战模型，其外在的形式是一个由节点和链路所组成的集合。节点是作战过程中的基本元素，主要包括传感器、信息处理中心、决策者、武器平台及目标等。以下是模型中节点的定义及其作用的描述。

**传感器（S）：**传感器是将检测感受到被测量的信息按一定规律变换成为电信号或其他所需形式的信息输出，以满足信息的传输、处理、存储、显示、记录和控制等要求的器件或装置的总称。如卫

星、无人机、侦察车等，本文中将侦察分队也抽象为传感器。在本文的分布式网络化作战模型中它用来接收来自其他节点的可观测信息，并把这些信息发送给信息处理中心。

**信息处理中心（I）：**用于融合、处理、分发信息的平台或系统。如指挥控制系统、情报侦察系统、勤务保障系统、火力支援系统、指挥车等。其作用是融合来自传感器的信息，对其进行相应处理后分发给相关决策者。

**决策者（D）：**作战中根据已知情报分析战场形势、作出作战方案、定下作战决心的指挥官或指挥机构的总称。其作用是接收来自信息处理中心的信息，并就节点的部署和作战的行动做出决策。

**武器平台（W）：**具有攻击敌方目标能力的战斗平台，如坦克、火炮、导弹等。本文中将执行作战任务的分队也抽象为武器平台。其作用是接收决策者的指令，攻击目标及与其他节点相互作用。

**目标（T）：**所有敌方具有军事价值的节点包括其传感器、信息处理中心、决策者和武器平台。

**链路**是节点之间的连接。链路根据其所表示的物理意义或的不同而分为多种类型，例如目标所发出的红外、电磁或可见光等信息被传感器探测到，这个过程就是一种链路。传感器探测到的信息被传送至信息处理中心，经处理后的信息分发至决策者，这种通信过程是另外一种链路。决策者向传感器、信息处理中心及武器平台发出指令，这些指令也被定义为链路。在信息时代的战斗模型中，链路不仅表示节点之间那些基于通信关系而建立起来的连接，而且代表节点之间在战术意图驱动下的作战行动，如武器平台攻击目标，这种攻击行为也是一种链路。另外，连接节点的链路是具有方向性的，本文中我们规定链路的方向为它所连接的两个节点

之间信息流向。

3 模型的作战效能分析

3.1 典型作战实例

美军数字化合成营是数字化机步师的基本作战单元，它具备整体的独立作战能力，是实施地面突击的基本作战力量，美军数字化合成营力量构成如图 1 所示，它由营部、2 个机步连、2 个坦克连和 1 个 120 自行迫榴炮连构成。其中，营部由 1 个指挥排、1 个综合保障排、1 个汽车班和 1 个炊事分队构成；机步连由 3 个机步排构成，每排 3 个机步班；坦克连由 3 个坦克排构成；120 毫米自行迫榴炮连由 1 个指挥排构成，2 个 120 毫米自行迫榴炮

排。为了验证所建立的分布式网络化作战模型的适用性，本文根据美军数字化营的编成情况建立其作战模型，并运用模型分析其作战效能。

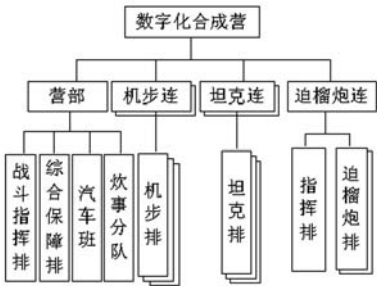


图 1 美军数字化合成营力量构成

根据上述美军数字化合成营的基本情况，对其建立如图 2 所示一个最基本的战斗网络模型。

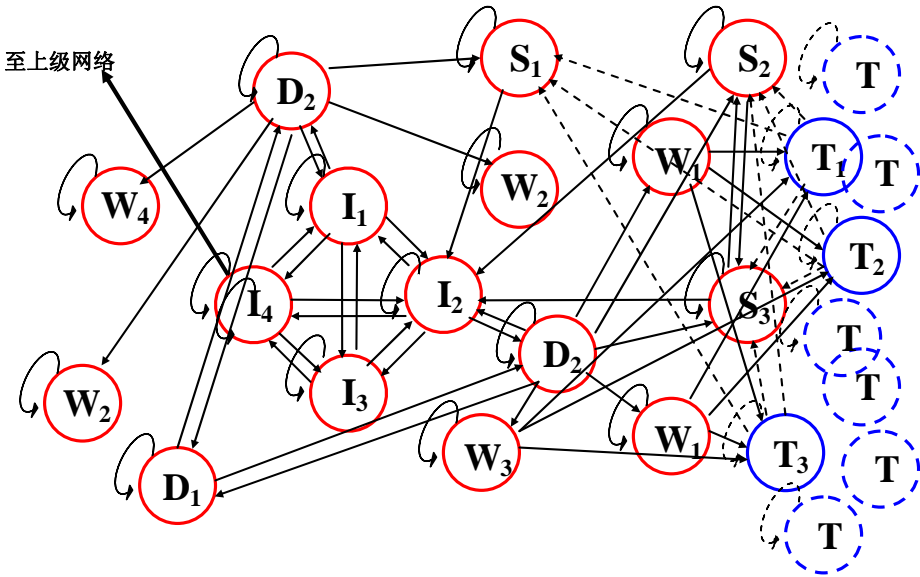


图 2 分布式网络化作战基本模型

图中 I1-I4 分别表示指挥控制、情报侦察、勤务保障、火力支援四个信息处理中心，这四个信息处理中心构成网状网以便实时交互信息并具有自愈抗毁性；W<sub>1</sub> 表示机步连，W<sub>2</sub> 表示坦克连，W<sub>3</sub> 表示迫榴炮连，W<sub>4</sub> 表示防空力量；D<sub>1</sub> 表示指挥员，D<sub>2</sub> 表示指控参谋；S<sub>1</sub> 表示卫星，S<sub>2</sub> 表示无人机，S<sub>3</sub> 表示侦察分队；蓝方 T<sub>1</sub> 至 T<sub>3</sub> 分别表示敌方信息处理中心、决策者、武器平台，虚线的 T 表示敌方其他各类有价值的军事目标。基本作战流程是：敌方目标 T 被我方传感器 S 探测到后将信息报告给信息处理中心 I，经处理后分发给决策者 D，决策者根据得到信息作出决策，并向武器平台 W 发出攻

击指令，武器平台接到指令后对敌方目标实施攻击。另外，己方 I、D、W 的位置信息也被 S 探测到，同样报 I 处理后送至 D，D 可根据战场的状况按需对其进行实时调整。

3.2 环的作战效能

环是指网络中的环路，它是一种由链路与节点组成的首尾相连的特殊结构，如图 2 中的传感器到信息处理中心到决策者到武器平台到目标再到传感器的环路。在上面的环路中，传感器发现敌方目标后将该信息传到信息处理中心，经合适的处理后报告给决策者，决策者作出作战的决定并命令武器平

台攻击目标, 攻击的情况再由传感器重新经该环路报给决策者, 决策者根据攻击情况制定下一步的作战方案, 完成一次完整的作战过程, 如果这个环路在任意一处中断, 就不可能成功地完成作战行动, 所以可以说正是因为作战网络中的环路的存在, 人们才能完成观察、判断、决策、行动的循环, 才使网络产生了战斗的价值。因此, 分布式网络化作战的优势也只能从这些动态的、复合的环中产生。尽管在理论上允许网络中存在只包含一个或两个节点的环, 但是这样的环在网络化的作战中用处很小。脱离战斗网络的单个传感器虽然也是一个子网, 但是除非将其连接到更大的战斗网络中, 否则该传感器并没有多大价值, 同样一个简单的目标-传感器环的用处也不大。三维以及更高维数的环才是产生网络化作战效能的源泉。

分布式网络化作战模型一般应具有控制环、催化控制环、催化竞争环和战斗环四种类型的环, 这四类环是构成其他复杂环的基础。本文以战斗环为例, 分析美军数字化营的作战效能。战斗环用于描述交战双方执行了作战行动。图3中的战斗环中, 我方传感器  $S_3$  探测到敌方目标  $T_3$ , 并将该信息送至信息处理中心  $I_2$ , 经  $I_2$  处理后报告给决策者  $D_2$ ,  $D_2$  命令我方  $W_1$  攻击敌方  $T_3$ , 传感器  $S_3$  监测打击过程, 监测到的信息经  $I_2$  再报告给  $D_2$ , 从而构成完整的环。

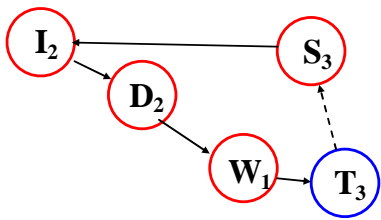
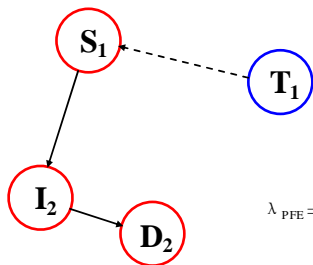


图3 战斗环

特征值是一个矩阵计算的数值, 是矩阵的一种综合参数。分布式网络化作战模型可以用邻接矩阵



$$\lambda_{PFE} = 0$$

图5 无环网络

的形式表示。图2的邻接矩阵表示形式如图4所示, 图中仍以不同颜色区分敌多双方节点, 从行节点到列节点如果有链路则在矩阵中用1表示, 否则用0表示。例如, 从图中可以看出敌方  $T_1$  到敌方  $T_2T_3$  之间没有链路(矩阵中该处数值为0), 敌方  $T_1$  到我方  $S_1S_2S_3$  之间有链路(矩阵中该处数值为1)。因为这种邻接矩阵恰巧是一种“稀疏非负矩阵”, 所以由Perron-Frobenius定理可知: 矩阵至少存在1个大于所有其他特征值的、实的、非负特征值。邻接矩阵为0—1矩阵, 该Perron-Frobenius特征值(PFE)有三种不同的取值, 而这三种不同值正好对应于网络化效能的三种度量: 无环网络、单环网络以及具有网络化效能的网络0。所以我们可以利用网络的邻接矩阵的特征值(PFE)来度量某一网络的网络化效能。

	$T_1$	$T_2$	$T_3$	$S_1$	$S_2$	$S_3$	$I_1$	$I_2$	$I_3$	$I_4$	$D_1$	$D_2$	$W_1$	$W_2$	$W_3$	$W_4$
$T_1$	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0
$T_2$	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0
$T_3$	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0
$S_1$	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0
$S_2$	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0
$S_3$	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
$I_1$	0	0	0	0	0	0	1	1	1	1	0	1	0	0	0	0
$I_2$	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	0
$I_3$	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0
$I_4$	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0
$D_1$	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
$D_2$	0	0	0	1	1	1	1	1	0	0	1	1	1	1	1	1
$W_1$	1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0
$W_2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
$W_3$	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1
$W_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

图4 邻接矩阵

图5的左半部分描绘了一个无环网络, 它不存在从一个节点出发还能够回到该节点的链路。图的右半部分是该无环网络的邻接矩阵, 该矩阵的PFE值为0, 因此, 这类无环网络不具有网络化效能。

	$T_1$	$S_1$	$I_2$	$D_2$
$T_1$	0	1	0	0
$S_1$	0	0	1	0
$I_2$	0	0	0	1
$D_2$	0	0	0	0

图 6 表示的是一个简单环网络，即一个没有后向反馈及前向反馈捷径的环。由于该网络中没有复

合的环，也就没有复合的网络化效能，该网络的邻接矩阵 PFE 值恰好等于 1.0。

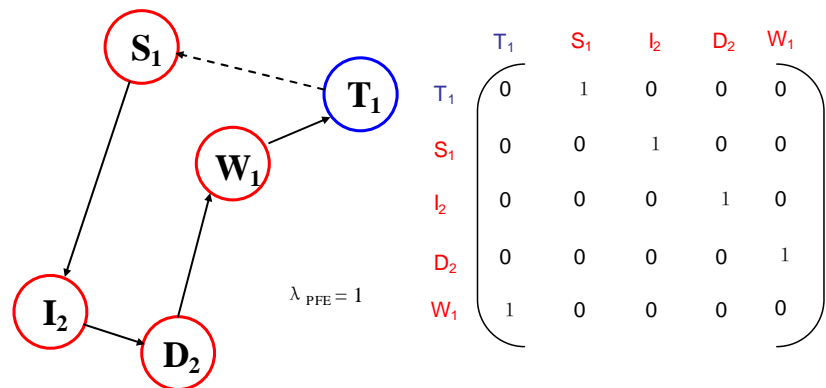


图 6 简单环网络

图 7 表示的是一个具有复合网络化效能的网络。与图 6 相比，它增加了一个传感器节点及相应的链路。由该网络的邻接矩阵的 PFE 值为可知，

增加的节点和链路形成的后向及前向反馈机制使该网络产生了网络化效能，可得到其特征数值  $\lambda_{PFE} = 1.14870$ 。

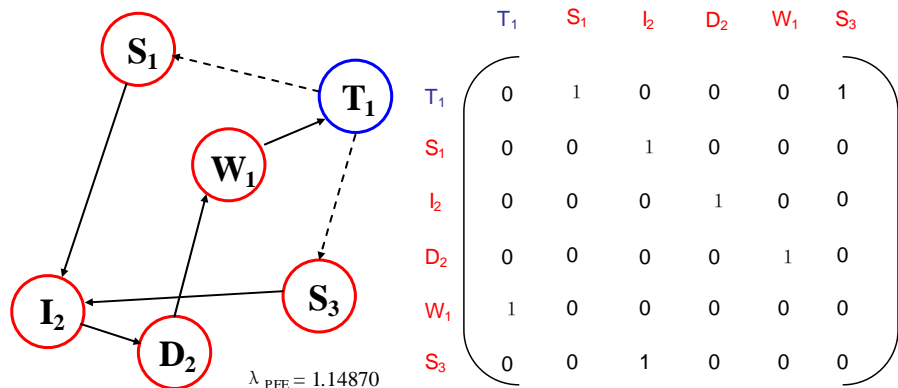


图 7 具有复合网络化效能的网络

3.3 模型的赋值

前面已经建立了分布式网络化作战模型并对其进行了分析，但在实际的作战条件下，不同的武器平台对同一目标实施攻击其效果是不一样的，同一武器平台对不同目标的攻击效果也不一样，而在采取不同的策略时，同一武器平台对同一目标进行攻击其效果同样是不一样的，也就是说采用不同的作战网络结构所能取得的作战效果是不同的。因此，如果不对模型中的链路赋以有意义的值，那么这个模型只能具有理论上的意义，而无分析实际问题的能力。

要对模型的网络化效能进行定量分析需要对模型中的链路进行赋值，本文规定：

链路的价值系数=（源节点价值系数+终节点的

价值系数）/ 2

模型中的节点按其在模型中所扮演的角色可分为五类，分别是传感器类、信息处理类、决策类、武器平台类和目标类。为使各类节点的赋值更加准确，更有意义，我们采用德尔菲法（专家咨询法）对各类节点进行评估。即将模型中所用到的所有节点分好类，然后根据不同类别节点的主要特征列出其各项性能指标并做成表格。之后将表格分寄给二十位以上军事专家，请专家根据自己的经验对每一节点的每一性能指标进行对比打分，分值采用百分制，最终得到每个节点和链路的价值系数。

仍用通过计算矩阵特征值的方法来比较引入价值系数后网络化效能的变化。在图 8 和 9 中，矩阵的含义与前述有所不同，如果从行节点到列节点之间没有链路则矩阵中用 0 表示，如果有链路，则根

据前面所述的专家系统得出该链路的价值系数。在图 8 中, 只用机步连 ( $W_1$ ) 对目标实施攻击, 在图 9 中用机步连和迫榴炮连 ( $W_3$ ) 共同对目标实施攻击, 经对二者矩阵的特征值进行计算可得, 图 9

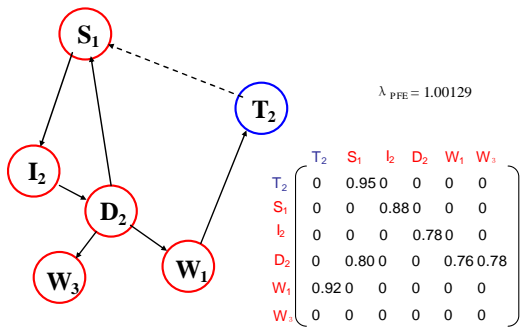


图 8 用机步连攻击目标时的网络化效能

的网络化效能要大于图 8。显然, 两种武器平台共同的攻击效果要大于单个武器平台的攻击效果, 这与我们的计算是相符的。

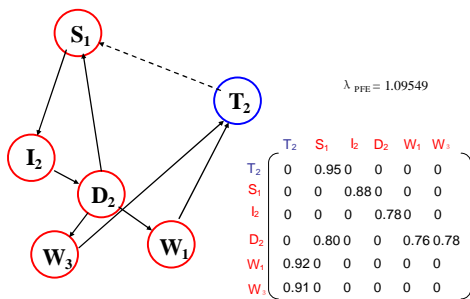


图 9 用机步连和迫榴炮连共同攻击目标时的网络化效能

4 结束语

本文在分析了分布式网络化作战特征的基本基础和一般规律基础之上, 结合复杂同网研究的相关理论, 用数学方法建立和描述了适应信息化条件作战的分布式网络化作战模型, 并以美军数字化营为

实例, 通过模型分析了分布式网络化作战网络化效能产生的机制, 对分布式网络化作战效能进行了评估与分析。对如何建设适应信息化条件的分布式网络化部队及如何充分发挥分布式网络化作战效能等问题进行了有益的尝试。

参考文献

[1] 陈太一, 信息战·数字化部队与数字化战场, 中国电子学会, 解放军通信工程学院, 总参第六十一研究所, 1998.5  
[2] 费爱国, 王新辉. 网络中心战效能度量. 北京: 军事科学出版社, 2004.5  
[3] 于全, 杰夫·凯尔斯. 分布式网络化作战—网络中心战基础, 2006.11  
[4] 詹姆斯莫法特. 复杂性理论与网络中心战  
[5] C. Eklund et al., "IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access, " IEEE Communications Magazines, June2002, pp. 98–107.

作者联系方式

通信地址: 武汉市解放公园路 45 号通信指挥学院 20 队  
邮政编码: 430010  
联系电话: 027-65021988

# 装备保障信息集成平台框架构建技术研究

卢洪义 王文双 史佩 应新永

**摘 要:** 目前,在装备保障信息化建设中,由于各部门、各机构的业务和功能归属不同,各单位建立了大量不同的、孤立的、异构的信息系统,成为制约装备保障信息化建设的瓶颈。弃之不用重新开发将会造成资源的极大浪费,通过建立一个通用数据库中间件,在系统业务逻辑、通用构件服务和数据源之间建立一个中间层,屏蔽各种异构数据源的差异,实现了在现有信息系统基础上的信息综合集成,为装备保障信息集成平台构建框架。

**关键词:** 装备保障; 信息集成平台; 框架构建

战争实践证明,装备保障是最终夺取战争胜利的关键因素,是维持和恢复战斗力的基本保证。现代高科技战争依靠的是高科技装备,装备战斗力的持续和恢复依靠的是科学的保障体系,在信息化条件下,科学保障体系的建设同样离不开信息化的支持。只有实现了信息化的保障体系,才有能力保障信息化作战条件下的高技术装备。

现代科学技术的发展,尤其是计算机网络技术、卫星通信技术等现代信息处理与获取技术的发展,使远程信息资源共享、实施纵深战略侦察成为可能,从根本上改变了传统的作战模式。所有的作战都必须依赖现代信息技术的支持,信息获取是完成一切作战任务的前提和关键。在信息战环境中,如何充分利用信息技术,实现装备保障信息化,提高对作战装备的保障能力,成了装备管理部门和各级技术保障部门工作中的关键问题。

装备保障各部门、各机构由于业务和功能归属不同,根据各自自身的需要,构建了许多相互隔离的异构的信息管理系统,他们之间的信息和业务都不一样,这就构成了一个巨大而复杂的异构数据库环境。如何集成、访问这些数据的关键问题是研究他们之间异构数据的集成问题,只有将这些孤立的数据都集成起来,提供给用户一个统一的视图,才有可能从巨大的数据资源中获取所需的东西。其次是选用合适的技术进行数据分析和处理。

## 1 信息集成平台需求描述综合模型建模

装备保障信息集成平台比一般软件复杂得多,

应用环境发生了很大变化,不能简单把一般软件开发的方法和技术移植到装备保障信息集成平台开发中去,需要运用新的方法和技术,建立装备保障信息集成平台的需求说明综合模型。

### 1.1 装备保障信息集成平台需求工程的难点

#### (1) 问题的复杂性

由于用户需求所涉及的因素繁多,而导致了问题的复杂化,因而要面对的问题是复杂化的问题。

#### (2) 交流障碍

装备保障信息集成平台需求工程涉及人员较多,如信息集成平台用户、保障领域专家、需求分析人员和平台开发人员等,这些人员往往具有不同的背景知识,又处在不同角度考虑问题,不可避免地造成彼此之间相互沟通的困难。

#### (3) 不完备性和不一致性

用户对问题的陈述往往不完备,其各方面的需求不可避免地存在着矛盾。需求工程的主要活动之一便是从初始的需求陈述中获取隐含信息,并消除其中的矛盾,最终形成完备且一致的需求定义,为后继开发打下基础。

#### (4) 需求易变性

用户需求的变动是一个极为普遍的问题,即使是部分变动,也往往会影响到需求定义之全部,从而可能会导致不一致性和不完备性。软件需求说明书采用的是形式化语言为主,半形式化语言为辅,形式化语言和半形式化语言结合的方法和技术,最后获得的是一份用形式化语言描述的完整的需求说明书。这种方法和技术对纯软件开发来说的确效果不错,但是装备保障信息集成平台不仅是软件要



素, 它还包括硬件、人和组织等要素, 其环境发生了很大的变化, 所以简单把软件开发的方法和技术移植到装备保障信息集成平台开发中去, 肯定会不适应。

## 1.2 装备保障信息集成平台需求描述综合模型

### (1) 平台初始状态获取

在需求说明处理的开始阶段, 对装备保障信息集成平台的认识还模糊不清。这个阶段只能寻求非常模糊的系统需求说明书, 参与需求分析工作的成员可由各方面的人员组成, 例如用户代表、平台开发维护人员、各级装备保障人员等, 由于专业背景不同, 所以对待建信息集成平台会有不同的理解。而且每个人都可能选择自己的表达方式, 有的采用自然语言, 有的采用草图、有的采用系统思想等等。但基本上是采用非形式化语言的描述方式, 所以平台需求说明书的初始状态是对集成平台认识的一个模糊视图。

### (2) 需求分析期望目标输出

需求分析的最终结果是希望获得一份待建平台的完整的需求说明书, 为平台开发的下一阶段使用。因此要求平台需求说明书具有可识别性和可理解性。为此, 初始状态的非形式化语言描述的方式, 要转化为统一的形式化语言来描述, 同时要求参与需求分析工作的成员对形式化的系统需求说明书达到共识。如果对平台需求说明书没有达到共识, 将在信息系统开发的后续阶段出现严重问题。

平台分析阶段的主要工作目标包括:

- 1) 将一个模糊不清的系统需求概念转换成一个完整的系统需求说明书;
- 2) 将非形式化描述转换成形式化描述;
- 3) 获得一份参与人员达成共识的需求说明书。

### (3) 综合模型

目前, 软件开发需求分析模型成熟应用的有三维模型和波浪式模型。三维模型将给定时期内对系统需求理解的深度、系统需求从非形式的语言描述到形式化语言描述的转换、对需求说明书从个人视角到共同视角的演化等三个不同的方面统一到一个动态的过程中; 波浪式模型反映了系统需求说明书获取过程的重复性, 演化性和并存性特点, 说明它是三维模型中动态演化过程形成任意曲线的主要原因。但这两个模型都是较为理想化的模型, 应用在

纯软件开发如操作系统、文字处理应用软件时效果非常好, 但应用在装备保障信息集成平台的开发时就不太理想, 因为信息集成平台比一个软件复杂的多, 平台的环境在不断变化, 装备保障的需求在不断变化, 装备保障人员的认识在不断变化, 平台是动态稳定的<sup>[1]</sup>。

把上面两个模型叠加在一起就可以建立一个客观反映平台需求说明的综合模型。综合模型既反映了平台需求说明书形成、演化的过程又说明了它演化的机制和原因, 为装备保障信息集成平台的下一步设计提供了一个比较可靠的前提。

## 2 装备保障信息集成平台集成策略

随着分布式应用的发展和普及, 多数据源集成及数据访问透明性问题已变得越来越重要。装备保障信息集成平台必须具有可扩展性, 可以实现数据源的“即插即用”, 这是传统的数据集成技术难以实现的。

在多家保障机构信息系统及辅助决策系统等项目的开发中, 发现涉及多数据源的系统有这样一个特点, 即整个系统开发都是围绕装备保障工作进行, 这些数据在具有相对一致性。因此, 可以建立一个通用数据库中间件, 通过在系统业务逻辑、通用构件服务(如事务、名字、安全等)和数据源之间建立一个中间层, 对服务层屏蔽数据源的差异。中间件向服务层提供一致的数据视图, 完成从实际数据源到用户数据视图的转换, 并在中间充当数据总线<sup>[2]</sup>。

XML 能够描述不规则数据, 能够从不同的来源集成数据, 将多个应用程序所生成的数据纳入同一个 XML 文件并传送到客户机上, 被解析出来的 XML 数据可以在本地被编辑或操纵。因此, 把 XML 作为集成层的数据描述工具和转换工具, 来构造数据集成的中间件, 不仅能装备保障信息集成平台的需要, 还将简化信息集成平台的实现。用户对信息的访问和操作不是直接作用于各数据源, 而是通过“虚拟数据库”来实现<sup>[3, 4]</sup>。通过 XML, 可以集成和统一来自不同或异质数据源的信息, 还可以为不同类型或持有不同设备(如固定计算机, 移动设备, PDA 等)的用户提供服务。

虽然文档具有数据存储管理的基本功能, 但是 DBMS 数据库管理系统比具有更加强大的数据管理

功能：数据存取的高效性；数据的一致性自动化保证机制；强大的数据完整性保证机制；多用户并发访问控制机制。所以目前在装备保障信息集成平台框架构建中，大量数据的存储管理还是依靠 DBMS 数据库管理系统，XML 的核心作用主要体现于共享数据的交换实现。

### 3 XML和DBMS数据库双向转换技术

在装备保障信息集成中，首先要将各级保障单位的信息映射为 XML 视图，并最终将经过转换后的 XML 视图映射到另一个装备保障单位的信息系统，由于 DBMS 数据库是企业信息数据的主要载体，就必然要求实现 XML 和 DBMS 数据库的双向转换。

将装备保障 DBMS 数据库映射为 XML 视图的方法为：首先获取 DBMS 数据库的具体关系模式，将具体关系模式再转换为一般关系模式，从一般关系模式中提取出表、字段、完性性约束等信息并通过有向图来表示。由于关系数据是由扁平的数据表构成，而 XML 是多层嵌套的层状结构，是由十三种模式组件组成的集合，通过定义模式组件与有向图属性的映射模板，实现数据库中表结构和相关属性的扁平结构到映射层状结构的转换。

装备保障上的 XML 视图反映到 DBMS 数据库的转换方法为：首先基于正则树理论对 XML 的数据结构与数据语义约束信息进行形式化描述，然后在 E-R 模型的基础上，通过建立 E-R 次序特性、引入父子元素的方向特性、扩展元素出现次数、建立附件信息等，形成扩展关系模型。通过建立 XML 形式化描述与扩展关系模型的元素与实体、元素到子元素与实体关系、属性等之间的对应关系，实现形式化描述到扩展关系模型之间的映射。通过将扩展关系模型转换为关系模式的数据结构，将扩展关系模型的约束条件信息转换为关系模式的数据约束条件，就可实现扩展关系模型到一般关系模型的转化，最后针对装备保障信息集成的具体 DBMS 数据库，实现一般关系模型的具体化，就可以实现 XML 向装备保障 DBMS 数据库的转换<sup>[5]</sup>。

## 4 面向应用集成的装备保障信息化平台框架

以装备保障领域现有的信息系统为基础，采用门户、数据交换、数据统计分析等技术，建立先进而完善的信息集成平台，为装备保障提供全面、及时的管理数据，实现装备保障信息化。

整个平台是基于分布式网络架构开发，基于统一的体系架构标准，建立统一的装备保障门户体系，利用数据交换平台将分散在各个技术流程中的数据提取出来，形成装备保障的中心数据库，进而利用数据统计分析系统，将隐含在数据背后的信息呈现在装备保障工作者面前，从而满足装备保障信息化的要求<sup>[6]</sup>。

应用整合解决方案的平台框架如图 1 所示。

在图 1 所示的应用整合解决方案平台框架中，自下而上分别包括如下几个方面。

数据库层：支撑装备保障信息集成平台的数据库，包括非结构化数据库、结构化关系数据库、工业部门 RMS 数据库以及装备保障单位现有数据库，这些数据源都由 DBMS 数据库管理系统管理。

数据交换平台：是装备保障信息集成平台的核心，用于建立与各应用系统、各数据库系统间的连接，并根据装备保障的需求提取数据形成装备保障中心数据库，并利用数据统计分析系统对中心数据库进行后续处理。中心数据库是一个“虚拟数据库”，它的建立过程是针对所有数据源数据模式的抽取过程，它将各应用系统数据库中的不同数据表示形式统一成一致的数据视图，应用系统和装备保障信息门户是针对虚拟数据库进行，与具体应用数据库无关。装备保障信息集成平台是面向各种信息源的，数据类型往往多种多样。由于 XML 具有可扩展性和结构性等特点，因此，采用 XML 模型作为信息集成平台的公共模型。

应用层：主要是装备保障全生命周期中各级保障单位的各个业务系统，既可以是现有的业务系统，也包括按照统一的装备保障信息化标准建立的新业务系统。

门户层：建立用户与装备保障信息资源之间的关系，将用户所需的信息、数据集中展示在一个统一的平台界面中，并支持实现各级装备保障业务系统间的单点登录。



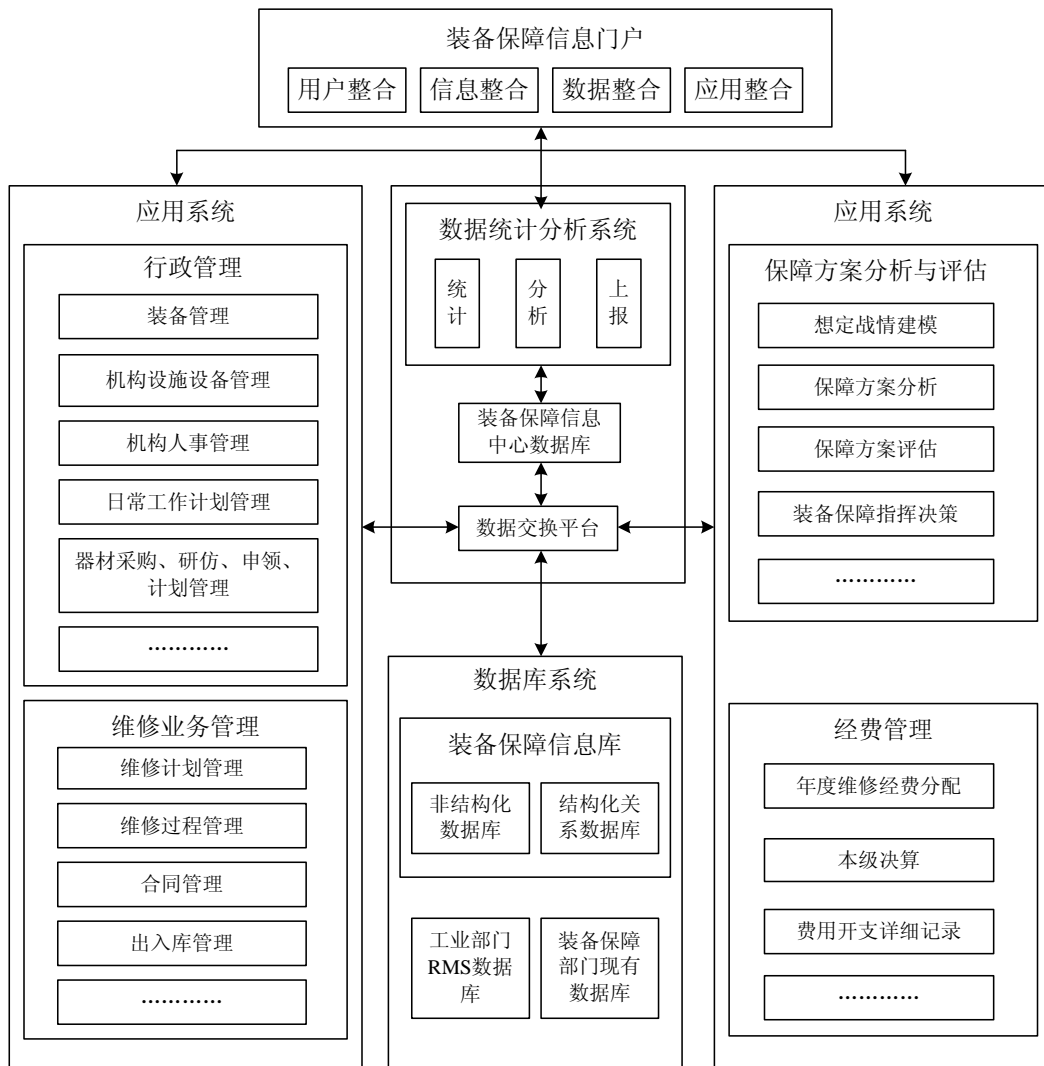


图1 装备保障信息集成平台总体框架

在以上应用整合解决方案平台框架的基础上，可以形成全新的装备保障信息集成平台体系架构，并在这一体系架构的基础上，实现装备保障全系统、全寿命周期原有业务系统间的信息整合、数据整合，支持跨系统的业务整合，同时为装备保障信息化平台的建设制定数据规范和接口标准。

### 参考文献

- [1] 罗伟其. 集成化信息系统需求描述的综合模型[J]. 小型微型计算机系统. 2003 (11)
- [2] 罗伟其, 姚国祥, 罗勇辉. 信息大系统的信息集成结构模型设计与实现[J]. 计算机工程与应用. 2001 (2)
- [3] 钱宇, 李相育, 李荷华. 基于 XML 和 Agent 的流程工业系统信息集成框架[J]. 计算机集成制造系统. 2001 (4)
- [4] 李军怀, 周明全, 耿国华, 张景. XML 在异构数据集成中的应用研究[J]. 计算机应用. 2002 (22)
- [5] 王东勃, 王润孝, 盛义军. 基于 XML 的供应链信息集成技术研究[J]. 计算机工程与应用. 2004 (10)
- [6] 周航滨, 夏安邦, 张长昊. 基于 Web 服务的跨企业信息集成框架[J]. 计算机集成制造系统. 2003 (1)

### 作者联系方式

通信地址: 山东烟台市海军航空工程学院

邮政编码: 264001

联系电话: 0535-6635559

# 国外防空反导武器系统网络化建设思路与途径分析

施荣

**摘 要:** 在分析了防空反导武器系统网络化所引发的优缺点后,介绍了国外防空反导武器系统网络化建设的思路,重点分析了国外防空反导武器系统网络化建设的思路。

**关键词:** 防空反导; 网络化; 混编防空反导; 爱国者; THAAD

## 1 引言

对于防空反导作战而言<sup>[1]</sup>,未来防空反导体系面临的是由多种空袭武器及其伴随的电磁干扰组成的复杂多变的一体化空袭体系。因此,未来的攻防对抗不是平台与平台之间的对抗,而是体系与体系、系统与系统之间的对抗。为适应这种整体对抗,必须打破传统的防空反导作战样式,综合集成各种防空反导作战资源,实现防空反导体系内各作战要素之间的信息共享和综合运用,以形成一个体系配套且多武器网络化作战的防御体系。

## 2 防空反导武器系统网络化的特点

实现防空反导武器系统之间以及防空反导武器系统与信息源之间的网络化已成为一种必然的趋势<sup>[2]</sup>。在没有连接的情况下,每个防空反导武器系统独立运作,不用考虑其他系统的存在。但在完全网络化的情况下,可联合制定防御计划,每个系统能够使用其他系统的资源。

网络化级别定义如下:1级是无计算机连接,协作仅仅通过语音通道实现;2级是通过计算机连接、外部提示机制和威胁信息共享算法,实现单一集成空景图;3级是通过计算机方式实现防御计划;4级是一个系统通过使用其他系统提供的数据制定防御计划并予以实施;5级是完全一体化,对其他系统的拦截弹实现集中决策、控制和制导。

实现防空反导武器系统的网络化可减少系统规模,扩大防御范围,提高杀伤概率,具有更好的强健性,可充分利用非建制传感器信息,与简单体系结构相比具有最低的费效比。

虽然实现防空反导武器系统的网络化具有诸多好处,但也必须看到由此所引发的问题。需要较复

杂的通信协议及定义算法和接口,将产生错误的航迹相关、错误的拦截方案等误差。网络化过程使参与系统产生大量要处理的数据,需要一定的投资,在整个费效比评估中增加的费用应与预期的好处权衡利弊。

## 3 国外防空反导武器系统网络化建设思路

### 3.1 探测器联网是防空反导武器系统网络化建设的基础

网络化防空反导武器系统分为探测网、信息网和交战网。其中,由所有战略、战役和战术级探测器组成的探测网通过数据融合等技术迅速合成整个战场空间的态势图,其完整性和精确程度远远超过任何单个探测器。作为网络中心战思想的提出者和海上网络化防空导弹系统的始创者,美国海军首先通过装备协同作战能力(CEC)系统把美国海军舰队的探测器连接成网络<sup>[3]</sup>。

CEC系统的主要设计思想是建立一个囊括战场所有探测器的网络。通过完全融合由位于不同地点的具有不同特征的探测器所提供的各种数据和信息,使所有单元能共享每个探测器的量测,这些单元得到的数据如同本地单元产生的一样。

CEC系统充分利用在不同地点的多个探测器和武器的整体能力,克服了单个系统的不足及其位置的局限性。如果CEC系统失去本地雷达航迹,但当航迹满足该单元的威胁交战准则时,作战系统将自动启动特殊的截获指示。通过CEC系统武器平台借助非建制探测器以及预警机或卫星的外部信息,扩大了目标探测范围,使舰船能够打击超出本地雷达视距的敌方目标,大大提高了区域、局部和自我防御能力。在全舰队内共享信息的模式将取代

传统的各自为战的海上防空作战模式,达到了真正意义上的协同作战,实现了网络化作战能力。

### 3.2 超视距拦截是防空反导武器系统网络化建设的前提

随着冷战的结束和濒海作战环境的出现,低空飞行巡航导弹的威胁越来越大,超视距拦截能力显得越来越重要。包括大型系留浮空器在内的大量传感器平台的使用舰载和陆基防空反导武器系统实现了超视距拦截。

1970年代,美国已开始考虑舰载导弹在机载平台的协助下拦截超视距低空飞行目标的概念,这种概念也被称为前向通过概念。1970年代中期,约翰·霍普金森大学的应用物理试验室(APL)负责研究了前向通过概念的最初版本。前向通过概念主要体现了超视距导引。标准导弹经舰载导弹中段控制链路导引接近F-14战机,经过改进的机载火控雷达照射目标,导弹实施半主动寻的。1980年代中后期,APL主要考虑用飞艇携带与宙斯盾巡洋舰上的相控阵雷达和照射装置功能相类似的一些武器系统,扩大对低空飞行巡航导弹的有效探测距离和作战距离。这些武器系统包括既可作为火控雷达又可作为照射装置的多功能相控阵雷达,该雷达提供了多目标照射能力,几枚SM-2导弹可同时进行寻的。此阶段的前向通过概念同时具有远程照射前向通过和协同作战能力,是基于远程数据交战的CEC系统的设计基础。这种基于远程数据交战模式允许舰船利用非本地的远程传感器数据发射SM-2导弹,并进行飞行中段制导和末段寻的照射。

目前,较为成熟的用于超视距拦截的浮空器方案是美国提出的联合对地攻击巡航导弹防御升高网络探测系统(JLENS)。

### 3.3 分布式无节点网络化结构是防空反导武器系统网络化建设的目标

防空反导体系已经历了三代体系结构,即单一火力单元防空、多层重叠覆盖和现在正在运用的分层集中控制体系。随着防空反导武器系统网络化进程的不断推进,防空反导体系将发展成为分布式无节点网络化结构。分布式指体系内各武器和设备可分布在一个大范围内的各空间点上,无节点指概念上没有传统的火力单元,即武器和设备之间在作战时没有固定必然的隶属关系,可根据目标、战场环

境、使用战术和部署情况,随时组合为具有从属关系的临时作战的网络化结构。

网络化结构内可包含多部各种类型的制导雷达、多部各类目标指示雷达、多辆各种型号的导弹发射车和多个作战管理指控中心。作战中对某个目标的拦截,可由某个确定的作战管理指控中心根据预警信息网提供的信息,指定体系内的几部雷达和几辆导弹发射车构成拦截系统对目标进行拦截,保证能用任何探测器发现目标,能用任何平台打击目标,实现利用最佳的武器攻击最适当的目标。

## 4 国外防空反导武器系统网络化建设途径

### 4.1 提高现有防空反导武器系统的网络化能力

为扩大防御范围,提高防御方案的灵活性,或在关键装备无法工作的情况下维持火力,通常要利用PAC-3系统的远程发射能力。远程发射能力是一项独特的旨在增强PAC-3系统发射能力的改进项目<sup>[4]</sup>,它允许发射车组部署在距离爱国者导弹连更远处。爱国者远程发射阶段1(RL1)能力允许发射站部署在距离作为爱国者导弹连的控制中心的交战控制站10km处,爱国者远程发射阶段3(RL3)能力允许至少由2个发射站组成的发射车组部署在距离有关的雷达装置30km处。爱国者RL3能力允许交战控制站控制1个本地发射车组和3个远程发射车组,当1个交战控制站的支援设备无法操作时,允许将远程发射车组的控制从本交战控制站转移到另一个交战控制站。

PAC-3/MEADS综合集成计划(CAP)旨在逐步将MEADS的主要成品(MEI)引入目前的PAC-3系统<sup>[5]</sup>,这种发展方法最终将实现MEADS目标能力。MEADS具有网络化、分布式、模块化的结构,目标MEADS连可根据作战需要进行调整,其BMC4I战术作战中心能与陆军和联合BMC4I结构集成,实现分布式系统作战和超视距交战,完全支持网络中心战和联合作战概念。预计于2015年进入系统研发和演示验证阶段和随后的低速始生产阶段,并将装备首个连级作战单元。

美国针对巡航导弹和无人机防御的作战需求,推出了21世纪霍克<sup>[6]</sup>。该系统是一种开放式、模块化、配置灵活以及易于升级的网络化武器装备。

发射单元既可以是霍克导弹发射单元,也可以是霍克和 SLAMRAAM 两种导弹的混编火力单元,或单一的 SLAMRAAM 发射单元。21 世纪霍克火力分配中心可与 SLAMRAAM、霍克、爱国者和近程防空系统实现无缝集成,具有完全互操作能力,能提供必需的计划功能和数据链,支持早期预警、目标识别、指示和交战。目前已交付 38 套,尚有 50 套处于合同生产阶段。

## 4.2 防空反导武器系统实现混编混配

自 2003 年以来,作为美陆军防空炮兵转型的最重大变化之一是撤销 6 个师属近程防空炮兵营和防空炮兵旅属复仇者防空营,由爱国者和复仇者混编防空导弹营作为美军未来地面防空的骨干力量。每个混编营装备 4 个爱国者发射连和 1 个复仇者连,能够有效地对付全方位的空中威胁<sup>[7]</sup>。

目前,美军正运用网络化火力概念使爱国者、SLAMRAAM、JLENS 等联成有效的作战网络。SLAMRAAM 系统通过采用陆军一体化防空反导系统探测器的数据,如哨兵增强型目标测距与识别雷达、JLENS 和爱国者雷达,将具有超视距拦截能力,使防空反导特遣部队能够对付现有系统拦截范围之外的各种威胁。SLAMRAAM 火力分配中心被美国陆军选作一体化火力控制站和下一代通用防空反导 BMC4I 的基准,它使作战实现完全网络化和分布式,并为未来发展提供了最大灵活性。

2010 年以前,防空炮兵部队将包括 8 个纯爱国者营、5 个防空反导混编营和 1 个纯 SLAMRAAM 营。这样,一个混编营就可完成以前两个营(近程防空营和中远程防空营)完成的任务,具备弹道导弹和巡航导弹双重防御功能。目前已组建了首批 2 个防空反导混编营。预计 2008 年底,美国陆军有望采用 24 个火力单元装备第 1 个 SLAMRAAM 营,2009 年 SLAMRAAM 将取代复仇者组成防空反导混编营。未来,随着 MEADS 逐渐取代爱国者系统,这些防空反导混编单元将由 MEADS 和 SLAMRAAM 组成。

参考文献(略)

作者联系方式

通信地址:北京市 142 信箱 15 分箱

邮政编码:100854

联系电话:13366063732 (张煜冲)

## 4.3 实现THAAD系统和爱国者系统的协同作战

美国的战区防空反导任务通常由 THAAD 系统和爱国者系统组成的防空反导特遣部队来完成。在执行防空反导任务中,THAAD 系统和爱国者系统可单独作战使用,但更多情况下,需 2 个系统形成高低两层防御体系协同作战来完成战区防空反导任务。防空反导特遣部队通常由在特遣部队战术作战中心(爱国者信息协调中心/战术指挥系统)控制下的 5 套爱国者火力单元和 1 套 THAAD 火力单元组成。

不管特遣部队采用何种组成或处于何种作战阶段,为充分应对空中和导弹的威胁,特遣部队作战必须实现一体化和协调。如果来袭战术弹道导弹能够分别由 THAAD 系统和爱国者系统拦截,则需要作战协调来优化使用拦截资源,并达到所需防御能力。在战术弹道导弹防御中,特遣部队战术作战中心为 THAAD 系统提供爱国者系统能力评估,以支持 THAAD 系统作战。当需要采用 THAAD 系统与爱国者系统协同交战时,THAAD 系统将发送确定是否需要低层防御支援。在作交战决策时,THAAD 系统计算交战火力方案,确定是否有足够的拦截资源来执行火力方案。一旦 THAAD 拦截弹的交战不成功,THAAD 系统将向爱国者系统发出警报。如果目标进入爱国者系统交战空域,并威胁到设防对象,则由爱国者系统进行拦截交战。

THAAD 系统将于 2009 年部署,初期将只部署 2 个连。战时根据需要,THAAD 连可直接编入防空反导营或爱国者导弹营。

## 5 结束语

防空反导武器系统网络化建设是以网络为中心和基础,使整个防空反导战场中的各种传感器、指控节点、武器平台等作战要素有机地集成为一个整体,提高整体作战效能。防空反导武器系统的网络化建设必将成为今后的重要发展方向。

# 信息化条件下装备保障模式初探

时和平 芮科慧 郝明

**摘 要:** 信息化战争由于其作战样式的改变而对装备保障工作提出了新的要求, 传统的装备保障模式已经不能适应信息战争条件下的装备保障。本文就信息化战争条件下装备保障问题提出了军地一体和军队各级协调一致的综合保障模式。

**关键词:** 信息化战争; 装备建设; 保障模式

随着科技的不断进步, 信息技术应用于军事领域已经越来越广泛, 引发了以信息技术为核心的军事革命, 战争的形态已经由传统的机械化战争转变为信息化战争。在信息化战争中, 武器装备的性能的发挥对于战争的胜负起着越来越大的作用。装备保障能够使得装备的性能达到最大, 这也就使得装备保障得到世界各国的重视。面对信息化战场, 装备保障的模式也必须根据作战样式的改变而有所发展, 本文就信息化条件下装备保障模式进行探讨。

## 1 信息化战争对装备保障提出新的要求

信息化条件下的装备保障, 是指为确保作战目标的实现, 以信息技术为支撑, 对各种保障力量和保障资源进行综合集成, 形成一个紧密结合的保障体系, 对所有参战装备实施的调配保障和技术保障活动。从概念可以看出, 信息化条件下的装备保障与传统意义上的装备保障在保障内容上没有实质性的区别, 但是在保障模式和方法上有很大的区别。信息化条件下对装备保障提出了新的要求, 主要表现为以下几个方面。

### 1.1 体系对抗激烈要求装备保障整体性高

信息化条件下的战争不再是各个作战单元之间的对抗, 而是体系间的对抗。就目前的指挥自动化系统而言, 它包括指挥控制分系统、情报侦察分系统、预警探测分系统、通信分系统、电子对抗分系统、以及其他作战信息保障分系统。它们之间互相制约、支持, 构成一个完的作战体系。对于系统中的任何一个分系统甚至使一些装备出了故障、被毁

等都会对整个作战系统造成巨大的影响。因此, 只有加强装备保障, 使各种武器都处于良好的状态才能发挥最大的作战效能。

### 1.2 作战节奏加快要求装备保障时效性高

信息化战争条件下战场高度透明, 作战进程空前加快, 必然要求战斗力能在有限的时间内急剧释放, 单位时间内武器、弹药、装备等作战资源的消耗量将成倍的增加。武器装备信息化程度高, 超视距精确打击已经成为现代信息化战争的一个主要特点。以美军的最近发动的几场战争为例, 在海湾战争、科索沃战争、阿富汗战争、伊拉克战争中使用的精确制导武器的数量占总数量分别为: 8%、30%、60%、80%。在这种无作战纵深的作战样式下, 抢修行动与战斗行动交织在一起, 弹药补充、抢修抢救极为紧迫, 损坏武器现场抢修、后送修理和物资器材补给的有效时间大大缩短。在这种条件下, 要求装备保障最大限度地实现各种装备保障资源, 尽量减少浪费, 优化配置、精确保障, 提高保障的实效性。

### 1.3 武器装备信息化要求装备保障人员素质高

由于科学技术的不断发展, 新技术不断应用于武器装备, 武器装备信息化程度越来越高, 结构越来越复杂, 受复杂环境、恶劣气候的影响就越大。而且由于超视距精确打击的实现, 武器装备受打击的部位、受损的程度、毁伤的模式与以往传统战争有所区别。由于受这些因素的影响, 装备保障的各种维修装备也由精密仪器、电子设备、计算机等组成。因此, 这也就要求有一支过硬队伍的保障来完成。

成信息化战场上的装备保障任务。在信息化战争中要建立一支由知识技术密集、指技合一的高素质人才组成的智能化保障队伍,才能满足信息化战争条件下装备保障的需求。

## 2 构建信息化条件下装备保障模式

信息化战争是全空域、全时域、全频域的战斗。战场情况复杂,前后方界限模糊,如果仅靠一种或两种保障模式很难及时、有效地完成保障任务。因此,为适应信息化战争的要求,就必须建立一体、综合的保障模式。

### 2.1 军地一体化保障

信息化战争不仅装备物资消耗巨大,而且战损率高,单靠军队自身的保障力量难以完成繁重的保障任务。军地一体化装备保障是现代信息化战争所必不可少的装备保障方式,从近期发生的几次世界局部战争中美军的保障经验看,建立军民一体的社会化保障体系,充分发挥了社会力量的巨大作用。军地一体化保障的优势主要体现在:

首先,地方保障力量能够为装备保障提供智力支持。随着信息技术的发展,技术的军用与民用的界限已经十分模糊,民用技术广泛利用于武器装备,这就为军民一体化保障的实现提供了可能。地方科技力量的投入可以为军队提供高素质的人才,以弥补由于装备信息化程度提高对装备保障技术人员要求的提高带来的人员培训不足等问题。同时还可以充分发挥地方高技术人才的作用,节约经费,减轻军队装备保障的负担。同时对于少数技术要求高,数量较少的装备要充分利用地方科研部门以及生产厂家的科研人员进行保障。

其次,地方保障力量的参与能够加快装备保障的速度,提高战时装备保障的实效性。信息化条件下的战争节奏快,消耗装备数量大,单靠部队来实现装备保障非常快难。地方保障单位的参与可以大大缩小战时装备保障的时间,使装备随时处于最佳的作战状态,发挥最大的作战效能。

同时,在实施军地一体化保障时要注意管理体制的建设,建立健全一整套军地一体化装备保障相应的法规,保障军地一体化装备保障的有效实施。

### 2.2 各级部队协调一致保障

信息化条件下的战争是系统之间进行对抗的战斗,军种之间的界限已经不存在,要求各军种协调一致作战,这也就要求建立打破军种界限的装备保障体系建立多专业,多层次优化组合,集中统一领导的装备保障体系,实施各个部队参与的综合保障。要充分利用好保障基地的统筹规划作用,实施就近、精确、跨军种的保障。要充分利用网络资源,战略级基地支援保障、战役级区域机动保障、战术级跟进伴随保障三者有机结合,相互衔接,最大限度地发挥整体保障效能。

### 2.3 装备保障模式构想

信息化条件下装备保障模式,应根据信息化战争的主要作战任务和作战样式,有利于各种装备保障力量主观能动性和创造性发挥,要有利于装备保障效能的最大发挥的原则选择保障模式。对于信息化条件下的战争,可以用“速度快、打击精确、高度透明”等几个词来概括因此,本文构建了这个统帅部、战区、作战部队与地方保障机构相结合的保障模式来实现信息化战争条件下的装备保障。其结构体系如图1所示。

图中,“ $\longrightarrow$ ”表示上级对下级装备保障的指挥,“ $----->$ ”表示上级保障机构对下级保障机构装备保障的指导,“ $\longrightarrow$ ”表示装备保障基地及机动保障部队对下级的支援保障,“ $\longrightarrow$ ”表示地方保障机构对装备保障的支援。

在这种综合装备保障模式下,由统帅部统一指挥、调配各个兵种和战区的装备保障力量统一进行保障;战区指挥作战部队进行统一保障。总部保障机构可以指导总部装备保障基地和机动保障部队进行保障;战区装备保障机构指导保障基地和机动保障部队进行保障;作战部队装备保障机构指导装备保障部(分)队。各级保障基地对下级保障基地或部(分)队进行保障支援。地方保障机构对各级保障部队进行支援,支援保障各级保障机构进行装备保障。这种集部队自身的保障力量和地方保障力量于一体的统筹规划的保障模式可以达到保障力量足、保障精度高、保障实效高的特点,适应信息化战争对装备保障提出的新要求。

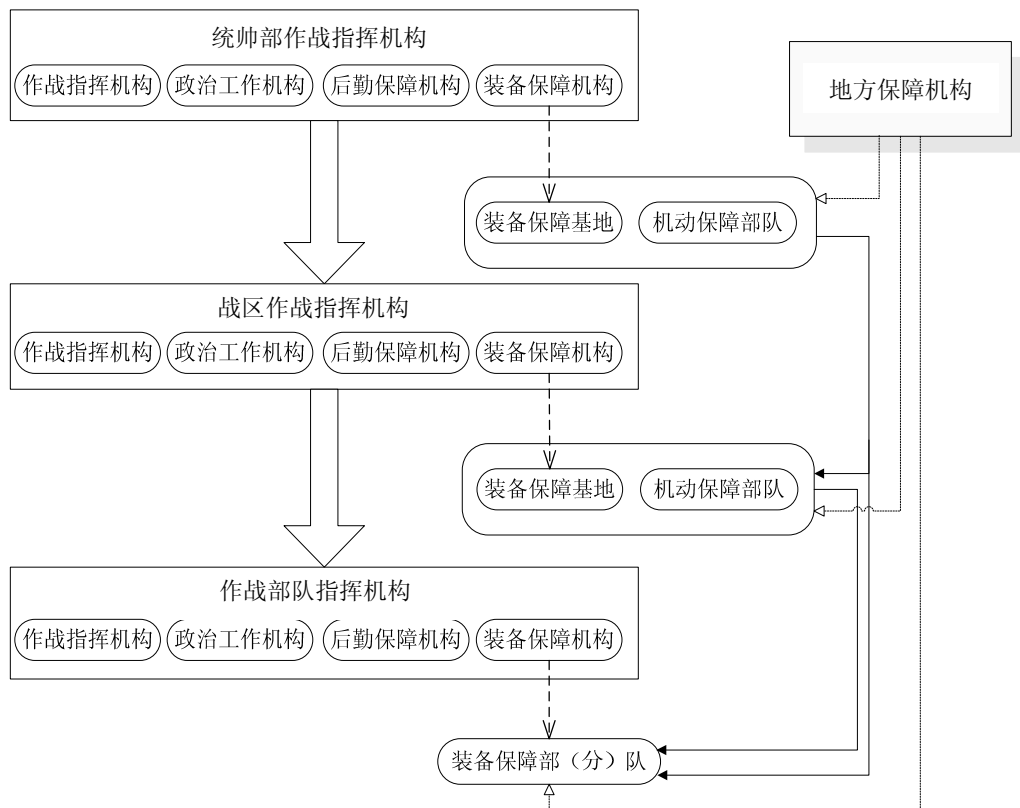


图1 装备保障模式图

### 3 结束语

随着信息技术的不断发展, 信息技术的军事化应用不断增加, 信息化战争的样式将不断出现, 这

就会对装备保障不断提出新的要求。装备保障要根据作战的需求而不断的发展新的保障模式。要把一切可能的力量应用于装备保障以适应信息化战争的需求。信息化战争必将催生了新的装备保障模式。

### 参考文献

- [1] 刘桂芳. 高技术条件下的 C<sup>4</sup>ISR—军队指挥自动化[M]. 北京: 国防大学出版社, 2003.7
- [2] 邢世忠, 陈达植. 军事装备学[M]. 北京: 国防大学出版社, 2000.11
- [3] 葛涛, 张玉柱. 加快装备保障信息化建设的几点思考[J], 装备技术指挥学院学报 2005 (2)
- [4] 张京乐. 适应高新技术武器装备发展推动舰船装备军地一体化保障[J], 装备 2007 (6)
- [5] 牛力. 信息作战指挥控制[M]. 北京: 解放军出版社, 2001.12

### 作者联系方式

通信地址: 西安市王曲镇西安通信学院

邮政编码: 710068

联系电话: 029-84706618

# 武警信息系统一体化技术体系结构的研究与制订

史国炜 王成海

**摘 要:** 文章首先论述了制订信息系统一体化技术体系结构的必要性, 然后介绍了制订《武警信息系统一体化技术体系结构》(WJ-ITA) 的相关背景, 最后在分析武警信息系统特点的基础上, 介绍了 WJ-IT 的主要内容和特点。

**关键词:** 武警信息系统; 一体化; 技术体系结构; 研究

## 1 制订信息系统一体化技术体系结构的必要性

从历史上看, 我国和世界一些发达国家一样, 在军事信息系统和电子政务系统建设的过程中, 都经历了独立分散、各自为战的开发建设阶段。在这个阶段, 政府各业务部门、军队各军兵种都是以自己特殊的应用目的为背景, 建立各自的应用系统, 由于缺乏统一的标准规范, 所建系统主要存在着如下一些问题。

- 1) 相互之间接口、协议、技术体制不统一, 信息互通困难。
- 2) 数据格式不一致, 难以实现及时高效的信息交换。
- 3) 数据描述不规范, 缺乏数据共享能力。
- 4) 人机界面设计随意性大, 容易导致误操作。

这种“烟囱式”的信息系统无法满足信息化条件下政府部门之间业务的协同, 也无法实现高技术条件下军队各军兵种联合作战的需要。而要改变这种状况, 发挥系统的综合效能, 就必须加强系统的顶层设计, 统一技术体制和标准规范, 把分散开发建设的信息系统综合集成成为一个有机整体, 保证各系统之间信息“无缝隙”流通, 实现系统互连、信息互通、功能互操作。

信息系统一体化技术体系结构是指, 为满足系统间的互操作性要求, 系统所必须遵循的技术标准、规范和协议的集合。科学合理的技术体系结构是信息系统顶层设计的重要内容, 可以为各类信息系统确立共同的技术参考模型, 提供统一的技术标准规范, 为信息系统一体化建设奠定基础。

## 2 制订武警信息系统一体化建设体系结构的相关背景

### 2.1 美军信息系统的技术体系结构

美国陆军最早展开了技术体系结构的研究, 95 年底制订了陆军技术体系结构 (Army Technical Architecture, 缩写为 ATA)。96 年美国国防部在 ATA 的基础上, 制定了美军的一体化技术体系结构, 并作为 C4ISR 系统体系结构框架 (C4ISR AF) 的一个组成部分。美军认为信息系统一体化建设的目标就是对其三军联合作战提供有效的信息支持, 因此, 其一体化技术体系结构被称作联合技术体系结构 (Joint Technical Architecture, 简称 JTA)。

JTA 是指导整个国防部信息系统建设和采办的高层文件, 美军称之为信息系统建设的“建筑法则”。JTA 规定了美国国防部各部局及军兵种在信息系统建设和采办过程中必须遵循的标准的最小集, 用以保证各种信息系统在联合作战条件下, 实现良好的互操作。随着技术的不断发展和新标准的出现, 美军投入了大量人力、物力和财力对 JTA 进行不断的补充和完善, 目前已升级为 6.0 版。

美军之所以制定三军统一的技术体系结构, 主要出于以下几个目的。

- 1) 为实现所有的战略、战术和战斗支持系统之间的互操作性奠定基础。
- 2) 为国防部系统开发和采办规定强制执行的信息技术标准和指南。
- 3) 向工业界传达国防部关于开放系统、基于标准的产品和实施的意图。
- 4) 确认工业界的以标准为基础进行开发的方



向。

5) 推动国防部面向网络中心战作战环境的转型。

## 2.2 我军信息系统的技术体系结构

在 20 世纪 90 年代末, 我军以军队信息化有关条令条例为指导, 在总结我军信息化建设经验的基础上, 参考和借鉴外军 C4ISR 系统建设的方法和成果, 展开了我军信息系统技术体系结构的研究, 并取得了实际成果。1998 年 3 月, 原指挥自动化局组织开展《指挥自动化系统互连互通互操作标准化研究》; 2001 年 5 月, 全军指挥自动化建设委员会办公室颁布《指挥自动化一体化技术体系结构》V1.0 版; 随着我军信息化建设的发展, 信息系统建设的范围比以往指挥自动化系统建设更加广泛, 为了进一步加强顶层设计, 为各类军事信息系统建设和综合集成提供统一的标准规范, 2004 年 8 月, 全军信息化领导小组对《指挥自动化一体化技术体系结构》进行了修订, 并更名为《军事信息系统一体化技术体系结构 (ITA)》, ITA 是“一体化技术体系结构”的英文缩写, 仍继续沿用, 版本号续排为 V2.0; 2006 年 4 月, 全军信息化领导小组再次对 ITA 进行了修订, 新版本为 V3.0 版。

我军制定 ITA 的目的在于:

- 1) 统一军事信息系统技术体制, 为实现系统互连、互通、互操作奠定基础。
- 2) 为诸军兵种军事信息系统一体化建设提供统一的标准。
- 3) 为装备研制和采购提供技术指南, 促进成熟技术在军事信息系统中推广应用。
- 4) 指导当前应急机动作战部队综合集成试点建设。
- 5) 指导研制单位系统地贯彻相关标准, 形成符合技术体制的产品和系统。
- 6) 导引新系统研制、老系统改造和系统综合集成, 提高效费比。

## 3 武警信息系统一体化技术体系结构的制订

### 3.1 武警信息系统的特点

全军 ITA 主要是针对我军作战指挥的一般特点和规律, 特别是针对我军履行国家防卫作战任务需

求而建立的技术架构。武警部队作为国家武装力量的重要组成部分, 其信息系统必然要具备军事信息系统一般的特点和规律, 如分层结构的划分、宏观模块的规划、通用性技术的采用等基本一致, 特别是在涉及系统互联互通标准上, 要大量采用 ITA 明确的标准和技术。然而, 武警部队履行职能的武装执法性、担负任务的艰巨复杂性、兵力部署的高度分散性、接触社会的广泛普遍性和领导指挥体制的军地双重性等特点, 决定了其在作战目标、作战样式、战术手段、指挥流程等方面与军队有着诸多的不同, 因此其信息系统从军事需求开始, 就与军事信息系统有着较大的不同, 这导致系统在分析、设计、建设等诸方面与 ITA 的要求有着明显不同, 这些不同主要表现在如下几个方面。

1) 武警部队双重的领导体制决定了其信息系统不仅要与军队系统互连互通, 还要与国家信息基础设施高度整合, 并要满足与政府电子政务系统、公安部门信息系统、目标单位信息系统的互通性要求, 因此在采用的标准上, 不仅要涉及军用标准, 还要涉及大量国家标准以及公安等行业标准。

2) 武警部队主要担负维护社会稳定、保障人民群众安居乐业的使命任务, 与军队的使命任务不同, 这就决定了武警信息系统并不过多涉及对武器系统的操作与控制, 而是主要涉及现场感知、指挥控制、安全防范、辅助决策等信息处理。

3) 武警部队兵力部署的分散性以及“战略层决策、战役级指挥、战术级行动”的作战样式, 决定了其信息系统在指挥作用跨度上更为广阔、在信息采集和处理上则更侧重微观战术级信息 (如小区域大比例尺数字地图信息、单兵信息等)。

4) 由于武警信息系统面向执勤、处突、反恐等中心任务, 因此要在确保支撑层技术标准相统一的同时, 还要对业务层进行“分类建设、分类指导、一体化使用”, 对不同勤务类型的信息系统甚至要采用“专勤专建”的方式。

### 3.2 WJ-ITA的制订

2005 年 1 月, 为适应武警部队执勤、处突、反恐等中心任务的需要, 在充分借鉴我军和外军技术体系结构的基础上, 结合武警部队信息化建设的实际以及武警信息系统的特点, 武警部队信息化领导小组制定并颁发了《武警信息系统一体化技术体系结构》第一版 (简称 WJ-ITA V1.0)。2007 年, 为适应部队信息系统建设需求的变化和新技术的发展, 武警部队信息化领导小组对 WJ-ITA 进行修改

和完善，形成了《武警信息系统一体化技术体系结构》第二版（简称 WJ-ITA V2.0）。和全军 ITA 相比，WJ-ITA 所选的标准更多，范围也更广，具有武警部队的特色。WJ-ITA 是武警部队信息化顶层设计的重要组成部分，确定了武警信息系统的技术参考模型，明确了为实现系统互连、互通、互操作，各部门应共同执行的一套技术标准。下面主要介绍 WJ-ITA V2.0 的内容和特点。

3.2.1 WJ-ITA V2.0 的技术参考模型

WJ-ITA 着眼加强顶层设计和统一技术标准，将研究对象与发展目标、应用环境、技术体制、管理要求等有机结合，制定完善了武警信息系统的技术参考模型（Technical Reference Model，缩写为

TRM）。TRM 是从建立一体化信息系统的角度出发，对各类信息系统的抽象化描述。其目的是建立一种适用于不同层次、不同类型的信息系统概念性框架，以科学地规范一体化技术支撑、应用服务和接口标准，为各类信息系统研制开发和装备订货的提供依据和指导。建立技术参考模型，有利于实现数据独立于应用，应用独立于平台；有利于提高软件的可移植性和可重用性；有利于建立真正的开放系统环境，提高系统的互操作性。

TRM 定义了业务应用层、基础应用层、应用支撑层、硬件实体层、外部环境等 5 个功能层以及应用程序接口（API）、外部环境接口（EEI）、硬件环境接口（HEI）等三类接口（见图 1）。

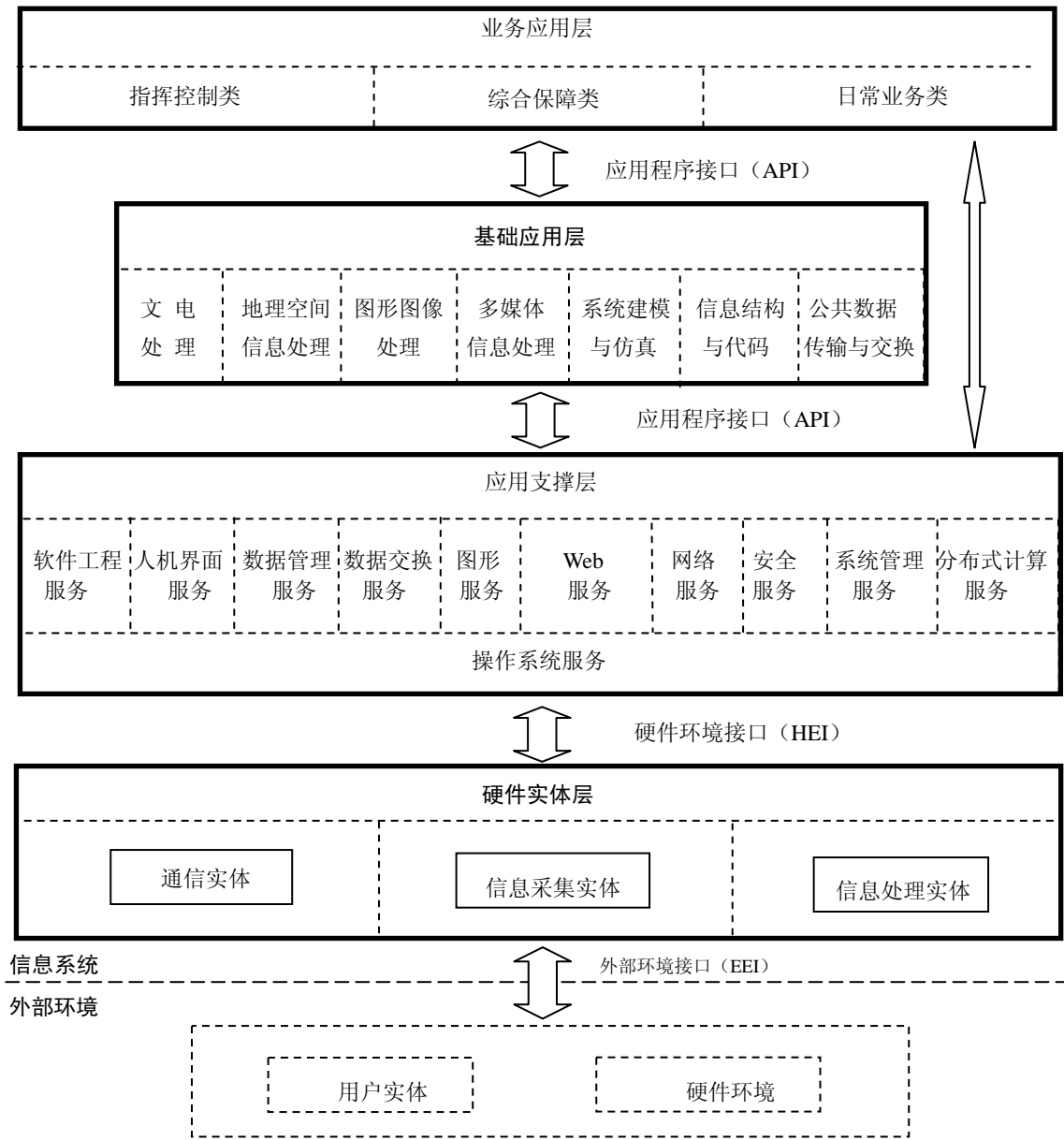


图 1 武警信息系统技术参考模型

和全军 ITA V3.0 相比, WJ-ITA V2.0 技术参考模型的调整主要包括以下 5 个方面。

1) 依据《武警部队信息化建设规划(2006-2010 年)》, 将业务应用层划分为指挥控制、综合保障、日常业务等三个功能模块。

2) 对信息系统的内外边界进行了重新界定, 将原来的外部环境层细分为硬件实体层和外部环境两部分, 把硬件实体层归在系统内部。

3) 硬件实体层除包括原有的通信实体和信息处理实体外, 增加了信息采集实体; 外部环境则在原有的用户实体的基础上, 增加了硬件环境方面的内容。

4) 功能层之间的接口除保留原来的应用程序接口(API)和外部环境接口(EEI)外, 在硬件实体层和应用支撑层之间增加了硬件环境接口(HEI), 从而将层间接口由两类扩展为三类。

5) 考虑到目前 Web 服务技术已由应用性技术发展为支撑性技术, WJ-ITA V2.0 将 Web 服务功能模块从基础应用层调整到了应用支撑层, 并对其内容进行了扩充。

### 3.2.2 WJ-ITA V2.0 所选的技术标准

基于武警部队信息系统的应用特点, 和全军 ITA V3.0 相比, WJ-ITA V2.0 在技术标准的选取上作了较大调整, 主要表现在以下 6 个方面。

1) 随着武警部队信息化建设的不断推进, 武警部队逐步制订了一些信息化标准, WJ-ITA V2.0

对这些标准进行了积极吸纳。

2) 为与地方政府实现信息交换和共享, WJ-ITA V2.0 参照国家信息化工作办公室发布的《电子政务标准化指南》, 结合应用实际, 增加了电子政务系统方面的技术标准。

3) 根据武警部队职能使命的需要, WJ-ITA V2.0 增加了安全防范系统方面的技术标准。

4) 根据信息技术的发展, WJ-ITA V2.0 增加了可信计算、自动交换光网络(ASON)等新生技术标准。

5) 根据信息技术的发展, WJ-ITA V2.0 删除了 ITA V3.0 中与当前武警信息化建设需要不相适应的一些陈旧标准。

6) 根据武警部队职能使命的不同, WJ-ITA V2.0 删除了 ITA V3.0 中与武警信息系统建设相关性不大的技术标准。

概括起来, WJ-ITA V2.0 共明确了业务应用层、基础应用层、应用支撑层、硬件实体层和外部环境等方面的各类标准共 545 项(包括: 武警部队标准 20 项, 国家军用标准 209 项, 国家标准 120 项, 国际标准 51 项, 行业标准 64 项, 工程标准 13 项, 国外先进标准 68 项)。其中, 133 项标准为系统实现互连、互通、互操作必须严格执行的标准, 其他 413 项标准为参照性标准, 具有导向性, 部队可结合工作需要选择地贯彻实施。

### 参考文献

- [1] 《军事信息系统一体化技术体系结构(ITA V3.0)》, 全军信息化领导小组, 2006.4
- [2] 王成海、蒋晓元、林春晖, 《贯彻军事信息系统一体化技术体系结构 ITA V3.0 应把握的问题[J]》, 军队指挥自动化, 2006.3

### 作者联系方式

通信地址: 北京海淀区西三环北路一号 武警总部司令部通信部

邮政编码: 100089

联系电话: 13718032169 010-68794110

# 野战通信与指控系统装车集成设计技术研究

谈学超 张军刚 冯占远

**摘 要：**本文简要探讨了野战车载系统体系结构模型，较全面的论述了野战车载系统装车集成过程中涉及的相关设计技术。

**关键词：**车载系统；体系结构；装车集成

## 1 野战车载系统体系结构

野战车载系统典型体系结构参考模型见下图。

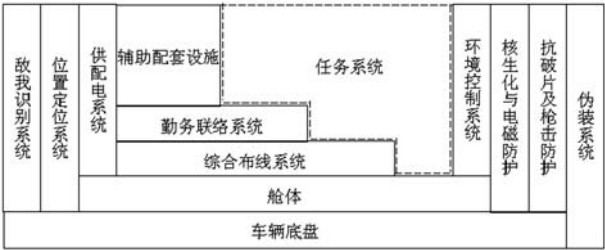


图 1 车载系统典型体系结构参考模型

野战车载系统根据其功能的不同可划分为任务系统和公用系统两大部分，如图 1 所示。其中任务系统是完成车载系统装备使命任务的主体部分，如车载通信系统、车载指挥控制系统。而公用系统是指各类车载系统都应具备的、用于支撑任务系统的子系统或分系统，即图 1 中除任务系统以外的其他部分。

## 2 野战车载系统装车集成设计技术分析

任何车载系统功能和战术技术指标的达成，均应通过详细技术设计的实现和相关关键技术的突破来保证。我们认为车载系统综合集成工作中应重点抓好系统布局设计、安全性设计、供配电系统设计、环境控制系统设计、电磁环境设计、可靠性设计、防护系统设计等几个方面的设计技术。

### 2.1 布局设计技术

#### 2.1.1 基本原则和要求

- (a) 经常操作的设备安装在工作人员方便操作的位置；
- (b) 质量与体积大的设备应安装在下部（如蓄电池组）；
- (c) 设备的分布应满足整车质心位置、前后轴荷分配、横向与纵向稳定性等车辆安全行驶的基本要求；
- (d) 设备颜色应相互协调；
- (e) 满足电磁兼容要求和人-机-环境工程要求。

#### 2.1.2 可采用的布局形式及特点

- (a) 集中布局  
将全部上装设备统一安装车内某一部位的布局方式。通常采用机柜进行安装。此种布局方式便于设备安装固定、线缆连接，方便操作；但受车辆质心分布限制，不利设备散热。集中布局一般可采用前置布局或后置布局方式。
  - (b) 分散布局  
将上装设备分别安装在车内两个或多个部位的布局方式。此种布局方式可以调整车辆质心位置，电磁兼容性好；但线缆连接、设备安装复杂，操作不方便。
- 对于车外布局，则应主要考虑整车运输超高超限及运输系留装置、采光窗设置、电源和信号孔口设置等问题。

### 2.2 安全性设计技术

车载系统安全性设计主要包括车辆行驶安全

性、电气安全性和防火防雷等。

### 2.2.1 行驶安全性

车辆行驶安全性应对整车重量、质心估算，前后桥轴荷分配，横向和纵向稳定性、抗风稳定性等方面进行设计和校核。

选择原点，建立合适的坐标系，确定舱体及各上装设备的重量及质心位置，可利用以下计算模型公式求取结果。

#### (a) 整车重量估算

整车总重量  $W = \sum W_i$ ，计算结果不应超过原底盘最大允许越野总质量。其中  $W_i$  为单个上装设备的重量。

#### (b) 质心位置估算

整车纵向质心位置  $X = \sum W_i \cdot X_i / W$ ，其中  $X_i$  为单个设备纵向质心位置；

整车横向质心位置  $Y = \sum W_i \cdot Y_i / W = c$ ，此为距对称中心左偏或右偏量。其中  $Y_i$  为单个设备横向质心位置；

整车质心高度  $Z = \sum W_i \cdot Z_i / W = H$ （距地面），计算结果不应超过产品规范要求。其中  $Z_i$  为单个设备质心高度。

#### (c) 轴荷分配计算

后桥负荷  $G_{后} = \sum W_i \cdot X_i / L$ ，计算结果不应超过原底盘规定的后桥最大允许总质量。其中  $L$  为轴距；

前桥负荷  $G_{前} = W - G_{后}$ ，计算结果不应超过原底盘规定的前桥最大允许总质量；

另外，根据 GB 7258-2004《机动车运行安全技术条件》的规定：“机动车在满载状态下，转向轴轴荷与该车最大允许总质量的比值不允许小于 20%。”，即  $G_{前} / W$  不应小于 20%。

#### (d) 稳定性校核

##### (1) 横向稳定性校核

考核方法 (1)：

根据 GB7258-2004 的规定：“车辆在静态状态下，向左侧或右侧倾斜的最大侧倾稳定角不得小于  $35^\circ$ ”。

侧倾稳定角  $\theta$  按下式计算：

$$\theta = \arctg \frac{B/2 - c}{H}$$

计算结果不应小于  $35^\circ$ 。其中， $B$  为两后轮

轮距， $H$  为质心高度， $c$  为质心偏离程度。

考核方法 (2)：

按照汽车力学理论，在水平路面上以等速等半径转向时不侧滑侧翻的条件为：

$$\frac{B/2 + c}{H} > \Phi, \quad \Phi \text{ 通常取 } 0.6.$$

##### (2) 纵向稳定性校核

考核方法 (1)：

车辆在  $30^\circ$  坡度上向上行驶时轴荷分布校核：

$$G_{后} = (W \times \cos 30^\circ \times X + W \times \sin 30^\circ \times H) / L$$

$$G_{前} = W \times \cos 30^\circ - G_{后}$$

其中， $X$  为质心与前轴的水平距离（即整车纵向质心位置）， $H$  为质心高度， $L$  为轴距， $W$  为汽车总重量。

根据 GB7258-2004 的规定， $G_{前} / (W \times \cos 30^\circ)$  的计算结果应不小于 20%。

考核方法 (2)：

按照汽车力学理论，下陡坡紧急制动不向前翻的条件为：

$$\frac{X}{H} > \Phi$$

其中， $X$  为质心与前轴的水平距离（即整车纵向质心位置）， $\Phi$  通常取 0.6。

##### (3) 抗风稳定性校核

抗风稳定性校核主要针对安装有抛物面天线的卫星车载系统。

天线风载荷  $\omega_{\text{天线}}$ ：为单位面积风载荷  $\omega$  与天线迎风面积  $A$  的乘积，即

$$\omega_{\text{天线}} = \omega \times A = (K_s \cdot K_H \cdot K_0 \cdot \omega_0) \times (\pi \cdot R^2)$$

其中  $K_s$  为风载荷体型系数， $K_H$  风压高度变化系数， $K_0$  风载荷调整系数， $\omega_0$  平面墙上的基本风压， $R$  为抛物面半径。

车厢风载荷  $\omega_{\text{车厢}}$ ：为单位面积风载荷  $\omega$  和车厢迎风面积  $A$  的乘积，即

$$\omega_{\text{车厢}} = \omega \times A$$

车辆在受风力载荷下的力矩为  $T_{\text{风}} = T_{\text{天线}} + T_{\text{车厢}} = \omega_{\text{天线}} \times H_{\text{天线}} + \omega_{\text{车厢}} \times H_{\text{车厢}}$ ，其中  $H_{\text{天线}}$  为天线质心高度， $H_{\text{车厢}}$  为车厢质心高度；

车辆自身力矩  $T_{\text{车}} = W \times H$ ，其中  $W$  为汽车总重量， $H$  为质心高度；

计算结果应为  $T_{\text{车}} > T_{\text{风}}$  才能足抗风稳定性要求。

### 2.2.2 电气安全性

车辆在停止状态下使用时应通过专用接地系统实现良好接地,当接地不良时应有声光告警;车辆在电源壁盒处应设计有避雷模块、漏电(包括电压型和电流型)保安器、过压和过流告警保护装置。

### 2.2.3 防火防雷

车辆内部和外部均应配备一套同时适用于扑救 A 类火灾、B 类火灾及带电火灾的灭火设备。同时应设计有感应雷电防护措施,电源线、信号线、天线馈线以及其他连线在舱体入口处应按具体要求安装避雷装置。

## 2.3 供配电系统设计技术

车载系统采用直流供配电体制,在设计过程中应详细统计各上装设备的功耗情况,计算出整车所需的直流功耗和最大交流功耗,据此选择合适的军用定型的发电机组和综合电源等设备,同时建立供配电系统连接实施方案。

### 2.3.1 供配电设备功率选择计算模型

车载发电机组和综合电源功率选择计算模型如下:

综合电源功率:  $P_1 = P_2 + P_3 + P_4$ ;

发电机组功率:  $P_6 = (P_1 - P_2) / \eta + P_5$ ;

$P_1$ ——综合电源输出功率;

$P_2$ ——暖风机功耗;

$P_3$ ——照明功耗;

$P_4$ ——其他直流负载功耗;

$P_5$ ——交流设备功耗(通常指空调);

$P_6$ ——发电机组输出功率;

$\eta$ ——综合电源效率(通常取 80%)。

注意,暖风机与空调不会同时工作,且空调功耗远远大于暖风机功耗。

### 2.3.2 供配电系统设计原则和要求

(a) 车辆供电优先次序:为市电-电源车-发电机组或自发电机-硅发与蓄电池组;

(b) 驻车工作时,优先由市电或电源车供电,

并通过车壁电源盒接入综合电源。此时也可由车载发电机组供电;

(c) 行进过程中,可利用车载发电机组或交流自发电机提供交流电,此时应直接接入综合电源。行进过程中不开启发电机组时也可由直流自发电机(或硅发)与蓄电池组共同为设备供电;

(d) 蓄电池组主要用于应急供电,实现直流输出不间断,支撑时间应不少于 30min。

## 2.4 环境控制系统设计技术

环境控制系统设计主要包括舱体通风换气设计、取暖设计、降温设计和照明设计等几个方面。

### 2.4.1 通风设计

车载系统有电磁屏蔽要求时,通常设计轴流风机进行舱内通风换气。

### 2.4.2 取暖设计

舱内取暖设备可采用独立式燃油空气加热器(暖风机)、电加热器或冷暖双用空调,取暖效果应满足 30min 内将舱内温度从  $-30^{\circ}\text{C}$  上升到  $0^{\circ}\text{C}$  以上的要求,同时舱内不应有异味和污染物排放;也可由底盘自带,取暖效果应满足原车要求。

通常根据热负荷计算模型选择相应热流量的暖风机。车厢制热量参考模型如下。

(a) 车厢热传导所致的耗热量

$$P_1 = K \cdot S \cdot \Delta T$$

其中,  $K$  为车厢热传导系数,通常取为  $2.0\text{W}/(\text{m}^2 \cdot ^{\circ}\text{C})$ ;

$S$  为车厢表面积 ( $\text{m}^2$ );

$\Delta T$  为车厢内外最大温差,通常取  $30^{\circ}\text{C}$ 。

(b) 换气扇换气时带入工作舱的冷量

$$P_2 = V_0 \cdot C_q \cdot (\rho_{T_{\text{外}}} \cdot T_{\text{外}} - \rho_{T_{\text{内}}} \cdot T_{\text{内}})$$

其中,  $V_0$  为风机的进风量 ( $\text{m}^3/\text{h}$ );

$C_q$  为空气比热,查得  $1004.304\text{J}/(\text{kg} \cdot ^{\circ}\text{C})$ ;

$\rho_{T_{\text{外}}}$  为环境温度  $T_{\text{外}}$  时空气密度 ( $\text{kg}/\text{m}^3$ );

$\rho_{T_{\text{内}}}$  为工作舱温度为  $T_{\text{内}}$  时的空气密度 ( $\text{kg}/\text{m}^3$ )。

(c) 车厢内设备及材料预热消耗的功率

包括钢、铝、泡沫、木材等预热消耗功率。

各种材料预热消耗功率可按式计算:

$$P = G \cdot (C_{\text{外}} \cdot T_{\text{外}} - C_{\text{内}} \cdot T_{\text{内}}) / \Delta t$$

其中,  $G$  为材料重量 (kg),  $C$  为材料比热 ( $\text{J}/(\text{kg} \cdot ^\circ\text{C})$ ),  $\Delta t$  为预热调节时间 (取为  $30\text{min}=1800\text{s}$ )。则车厢内总的预热消耗功率:

$$P_3 = P_{\text{钢}} + P_{\text{铝}} + P_{\text{泡}} + P_{\text{木}}。$$

(d) 车厢内空气预热消耗的功率

$$P_7 = CP \cdot \rho \cdot V \cdot \Delta T / Zt$$

其中,  $CP$  为定压比热, 取为  $1\text{kJ}/(\text{kg} \cdot \text{m}^3)$ ;

$\rho$  为空气比重, 取  $1.29\text{kg}/\text{m}^3$ ;

$V$  为车厢内部容积 ( $\text{m}^3$ );

$\Delta T$  为舱内外温度差 (取为  $10^\circ\text{C}$ );

$Zt$  为调节时间, 取为  $30\text{min}=1800\text{s}$ 。

由此, 可得出总耗热量  $P = P_1 + P_2 + P_3 + P_4$

(W)。

### 2.4.3 降温设计

舱内降温设备可采用军用空调器, 降温效果应满足当环境温度为  $40^\circ\text{C}$  时,  $40\text{min}$  内将舱内温度降低到不高于  $30^\circ\text{C}$  的要求 (夏季温度应能降到  $28^\circ\text{C}$ , 春秋季应能降到  $25^\circ\text{C}$ ); 也可由底盘自带, 降温效果应满足原车要求。

通常根据热负荷计算模型选择相应制冷量的军用空调器。车厢制冷量参考模型如下。

(a) 车厢热传导所致的耗冷量

$$P_1 = K \cdot S \cdot \Delta T$$

其中,  $K$  为车厢热传导系数, 通常取为  $2.0\text{W}/(\text{m}^2 \cdot ^\circ\text{C})$ ;

$S$  为车厢表面积 ( $\text{m}^2$ );

$\Delta T$  为车厢内外最大温差, 通常取  $10^\circ\text{C}$ 。

(b) 太阳辐射进入车厢的热功率

$$P_2 = K \cdot FP \cdot (T_m - T)$$

其中,  $K$  为车厢热传导系数, 通常取为  $2.0\text{W}/(\text{m}^2 \cdot ^\circ\text{C})$ ;

$FP$  为车厢向阳面的最大面积 ( $\text{m}^2$ );

$T_m$  为太阳照射下向阳面的平均温度, 计算时

取为  $T_m = T + 20$ ;

$T$  为车厢外环境温度。

(c) 车厢内电子设备的散热量

$$P_3 = n_1 \cdot n_2 \cdot n_3 \cdot n_4 \cdot N$$

其中,  $N$  为各电子设备最大输入功率总和 (W);

$n_1$  为安装系数 (设计功率与安装功率之比),

通常取 0.8;

$n_2$  为负荷系数 (平均功率与设计功率之比),

通常取 0.7;

$n_3$  为同时使用系数, 一般取 0.7;

$n_4$  为蓄热系数, 一般取 0.8。

(d) 车厢内工作人员人体散热量

$$P_4 = n \cdot q$$

其中,  $n$  为工作舱内工作人员的数量,  $q$  为单个人的散热量 (夏季), 通常取  $145\text{W}/\text{人}$ 。

(e) 换气扇换气时带入工作舱的热量

$$P_5 = V_0 \cdot C_q \cdot (\rho_{T_{\text{外}}} \cdot T_{\text{外}} - \rho_{T_{\text{内}}} \cdot T_{\text{内}})$$

其中,  $V_0$  为风机的进风量 ( $\text{m}^3/\text{h}$ );

$C_q$  为空气比热, 查得  $1004.304\text{J}/(\text{kg} \cdot ^\circ\text{C})$ ;

$\rho_{T_{\text{外}}}$  为环境温度  $T_{\text{外}}$  时空气密度 ( $\text{kg}/\text{m}^3$ );

$\rho_{T_{\text{内}}}$  为工作舱温度为  $T_{\text{内}}$  时的空气密度 ( $\text{kg}/\text{m}^3$ )。

(f) 车厢内设备及材料预冷消耗的功率

包括钢、铝、泡沫、木材等预冷消耗功率。

各种材料预冷消耗功率可按下式计算:

$$P = G \cdot (C_{\text{外}} \cdot T_{\text{外}} - C_{\text{内}} \cdot T_{\text{内}}) / \Delta t$$

其中,  $G$  为材料重量 (kg),  $C$  为材料比热 ( $\text{J}/(\text{kg} \cdot ^\circ\text{C})$ ),  $\Delta t$  为预冷调节时间 (取为  $40\text{min}=2400\text{s}$ )。则车厢内总的预冷消耗热功率为:

$$P_6 = P_{\text{钢}} + P_{\text{铝}} + P_{\text{泡}} + P_{\text{木}}。$$

(g) 车厢内空气预冷消耗的功率

$$P_7 = CP \cdot \rho \cdot V \cdot \Delta T / Zt$$

其中,  $CP$  为定压比热, 取为  $1\text{kJ}/(\text{kg} \cdot \text{m}^3)$ ;

$\rho$  为空气比重, 取  $1.29\text{kg}/\text{m}^3$ ;

$V$  为车厢内部容积 ( $\text{m}^3$ );

$\Delta T$  为舱内外温度差 (取为  $10^\circ\text{C}$ );

$Zt$  为调节时间, 取为  $40\text{min}=2400\text{s}$ ;

由此, 可得出总耗冷量  $P = P_1 + P_2 + P_3 + P_4 +$

$P_5 + P_6 + P_7$  (W)

### 2.4.4 照明设计

舱内应配备常规照明灯、应急照明灯和防空照明灯, 同时可根据需要配备移动应急照明灯。常规照明灯通常采用荧光灯或 LED 灯, 应急照明灯应由舱内其中一盏常规照明灯担任。

## 2.5 电磁环境设计技术

电磁环境设计包括电磁兼容设计、电磁屏蔽设计和综合布线设计等几个方面的内容。

### 2.5.1 电磁兼容设计

在进行系统电磁兼容设计时, 首先应详细分析电磁干扰方式、主要干扰设备及敏感设备、主要无线设备及干扰特性等, 综合考虑运用设备布局及布线技术、电源系统设计技术、车内接地系统设计技术、天线布局设计技术等, 实现整个系统相互兼容。

### 2.5.2 舱体电磁屏蔽设计

舱体是抑制外部电磁波进入车内的最重要环节之一, 其屏蔽效能好坏直接影响到车内各设备能否正常工作。在进行电磁屏蔽设计时, 应综合运用舱体结构设计、屏蔽门设计、屏蔽窗设计、信号孔口板与电源孔口板屏蔽设计、接地设计等相关技术, 以满足屏蔽效能等级要求。

### 2.5.3 综合布线设计

综合布线设计与系统电磁兼容和舱体电磁屏蔽的设计密切相关。综合布线设计包括电源系统布线设计、信号系统布线设计和车内接地系统布线设计等几个方面。

## 2.6 可靠性设计技术

可靠性是制约装备系统作战适用性、保障性和整体效能的重要因素之一。系统的可靠性指标与系统构成、系统典型任务剖面及系统寿命密切相关, 通常分为系统的基本可靠性和任务可靠性。应根据假设条件建立基本可靠性数学模型和任务可靠性数学模型, 进行系统基本可靠性预计和分配、任务可靠性预计和分配, 必要时还要进行可靠性调整和分配, 最终得出系统固有可用度, 比较计算结果是否满足战技指标的相关规定。

## 2.7 防护系统设计技术

车载系统防护设计包括伪装防护、抗打击防护、核生化防护等几个方面。

### 2.7.1 伪装防护

为避免或减弱被敌方探测和发现, 应设计相应的迷彩图案, 使车辆表面的涂覆能防近红外线探测; 车辆外部装设全波段伪装网, 完成系统任何状态下的隐蔽功能, 同时应在舱内应配置防空灯。

### 2.7.2 抗打击防护

抗打击防护设计主要指轮式越野汽车的抗破片及枪击防护设计。有要求时, 可通过外挂防护装甲板、采用防弹玻璃、使用低气压防弹轮胎等设计措施, 使车辆满足规定的防护要求。

### 2.7.3 核生化防护

车载系统有要求时, 应采用超压式集体防护形式。以人员的集体防护为主, 个人防护和装备防护为辅。舱体密封性应满足规定要求, 同时设计合理的集体防护装置和报警装置, 使系统满足规定的防护要求。

## 3 小结

车载系统集成不是任务系统设备和公用系统设备的简单堆积, 必须从整体任务使命出发, 进行充分的系统功能集成和整体优化, 使车载装备自身成为统一的整体。在车载系统研制工作中, 除了完成任务系统和公用系统的车载化装备形式转换外, 更重要的是通过装载设备的一体化集成, 实现车载形态装备实体的系列化、标准化和通用化。

### 参考文献

- [1] 总参第六十一研究所. 车载式野战系统装备体制及通信指控一体化装车方案论证, 2005.12
- [2] 智永红. 车辆改装稳定性的设计与分析[J]. 矿山机械, 2001.08
- [3] 董新发等. 专用车稳定性校核[J]. 专用汽车, 2006 (4)

### 作者联系方式

通信地址: 北京丰台大成路 13 号 S00

邮政编码: 100039

联系电话: 010-66820262



# 对临近空间军事开发利用的探讨

王传才 周义建

**摘 要:** 本文从临近空间军事应用入手,探讨了国内外对临近空间开发利用技术领域的现状,特别是美军正在实施的一些技术举措。提出了对临近空间开发利用的一些考虑,认为开发利用临近空间空域内的气球、飞艇以及滑翔机等各种平台,通过携带不同类型的载荷,以达到具备通信、遥测、情报、侦察和监视等各种军事用途。

**关键词:** 临近空间; 开发利用; 探讨

## 1 概述

临近空间近年来引起了各主要军事国家的特别关注,它作为未来空天一体作战的重要战略资源,特别是现代作战由空向天的发展趋势,它已经成为一个不可逾越的平台。因此,着眼未来军事斗争准备需要,加大对临近空间军事开发利用的研究,是顺应未来军事斗争发展的明智之举。

## 2 临近空间军事开发利用的价值

临近空间的开发利用主要是在此空间设置各类平台,即指工作于临近空间空域内的气球、飞艇以及滑翔机等飞行器。它们通过携带不同类型的载荷,具备通信、遥测、情报、侦察、监视和电子对抗等各种军事用途。美军认为,目前,在临近空间区域主要存在着两个军事应用的空白,一是缺乏持续的通信和情报、监视、侦察、电子战效能;二是军事作战武器没有覆盖这一高度,因此,要想在未来战争中立于不败之地,必须要重视对临近空间的开发利用,它是一个具有巨大军事价值的区域。

### 2.1 具有对“天”和“空”的补充与关键时刻的“替代”作用

采用多层的侦察手段可以使敌方难以实施相应的防范措施,把临近空间平台作为空载和卫星战略侦察能力的强有力的补充,能够承担部分空载平台的战略侦察任务。在战略防御任务中,美军设想将临近空间作为空间效能的备份,它们正在研究在丧失了 GPS 卫星导航能力的情况下,如何利用临近

空间平台进行 GPS 能力重构替代。从目前的发展状况看,临近空间的军事应用仍处于理论研究和概念验证阶段,但美国正在加快临近空间领域军事应用的步伐,有望在近期部署基于临近空间平台的军用通信系统以及侦察、监视遥感器。

由于临界空间空气稀薄,对飞行器的升力、阻力和发动机的推力影响很大,并且飞行器的操纵性和安定性也变很差,因此,大多数飞行器的升限都被限制在 10~30 千米之间,而 30~100 千米之间很少使用。而卫星由于受重力作用过大,难以维持其飞行轨道。但从另外一方面看,该区域气流比较稳定,空气流动相对较小,是部署高空悬停气球或飞艇的理想空域,也是未来型飞行器又一场所。从军事应用角度看,它相对卫星距离地面较近,如同样的侦察设备可以获得更高的分辨率,在该空间设置各类平台,具有能够获得更为真实、准确的信息,另外,绝大多数的固定翼战斗机和地对空导弹无法达到临近空间这一高度。在伊拉克战争中,美国陆军面临的情报、侦察和监视保障方面的需求矛盾日益突出,因而它们利用临近空间及其平台所具有的优势,在伊拉克部署了名为“快速初始部署浮空器”的侦察飞艇系统,使其地面部队更加快捷有效地获得了战场情报,并且取得了一定的作战效果。从以上我们可以看出,临近空间承上启下,是太空和空中的重要补充,是空天一体作战不可逾越的中间平台,其战略地位十分重要。

### 2.2 与“天”、“空”军事效益对比优势明显

临近空间平台在覆盖范围、分辨率、灵敏度、成本以及生存能力等方面都具有很大的优势,它们载荷有关设备,与卫星和飞机相比其最有效而且特

有的是长持续性能力。轨道力学本身限制了任何轨道上的单颗卫星在凝视型监视上的时间持续性，空载平台由于其燃料限制，最长持续时间也仅为几天，而临近空间平台通常采用悬浮气球或者飞艇，巡航速度低，滞空时间长，具有长达数月的滞留和监视能力。另外，从战术机动能力看，临近空间平台与卫星和飞机相比，可以充分发挥其快速反应、持续时间长和区域覆盖好的特点，圆满地完成通信、侦察和监视等战术任务。除了地球静止轨道卫星外，其他卫星不能长时间进行战场监视和侦察工作。保证监视、侦察的连续性覆盖就需要卫星星座间较多的星间切换，这就增加了卫星系统的复杂性，因此，对卫星而言执行战术任务是困难的，空载平台和无人机适合执行战术任务，持续时间长达数月，十分适于战场、战术应用。临近空间平台还有装备体积较小、质量轻等优点，战场指挥员可以配备具有多个临近空间平台及其相应载荷的支援分队，直接控制分队进行临近空间平台的部署，包括临近空间系统的发射、回收和整个任务执行期间的操作，从而获得快速、灵活的  $C^4ISR$  效能。因此，临近空间平台在战术任务应用中具有广阔的前景。临近空间极具军事应用潜力，在战场支持方面将发挥巨大的作用。

### 3 外军临近空间开发利用技术领域的现状与发展

美军认为，如果研制出一种能够在临近空间空域活动的作战武器，就会掌握极大的战场主动权，从而改变现有海陆空三军作战的模式，将战争引入更高的空间。目前，虽然临近空间开发利用还处在研究、论证和试验阶段，但由于其自身所具有的优势，使其具备了旺盛的生命力和良好的发展前景。美国积极围绕临近空间飞行器展开的开发利用，特别是对各种应用技术，加大了研究力度。

#### 3.1 加大飞行器平台技术研究

美军在高速临近空间飞行器方面，主要采用高超声速下的高升阻比气动外形、高超声速无动力滑翔或高超声速吸气式推进技术，有空间作战飞行器、通用再入飞行器、亚轨道飞行器等。这类飞行器一般无人驾驶、飞行高度高、速度快（数倍音

速）、升空时间短、攻击能力强，可进行天地往返运输和维修卫星等空间系统，还可用于摧毁敌方空间系统、拦截弹道导弹和对地进行精确打击等；在低速近空间飞行器方面，主要利用近空间空气的浮力和飞行器运动产生的升力，有高空无人机、高空飞艇、高空气球等。这类飞行器一般无人驾驶、飞行高度低、速度慢（亚音速）、滞空时间长（续航力强）、信息获取处理能力强，主要用于探测、侦察、情报收集、通信等。低速近空间飞行器平台涉及的技术非常广泛，其中关键技术包括：结构与材料、动力、飞行管理与控制及生存能力。

#### 3.2 探索各类军事应用载荷技术

美军认为，低速近空间飞行器的有效载荷种类繁多、形式各异，不同任务需要的载荷不同，面临的技术问题也有很大区别。总起来说，有效载荷的关键技术主要有信息获取技术和信息处理技术。在信息获取技术方面，低速近空间飞行器系统主要用于执行探测、侦察、情报收集、通信等任务，有效载荷信息获取的能力与质量直接关系到执行任务的结果与质量。传感器技术是信息获取的关键，传感器最主要的功能是成像（可视、红外和雷达）；其次是信号探测，包括探测化学、生物、放射性大规模杀伤性武器，气象海洋学的气象信息，反潜战和反水雷战中的磁信号等；在信息处理技术方面，美军认为低速近空间飞行器系统对信息处理技术的要求主要是处理速度快、容量大，算法准确经济，信息融合度高。处理器技术不仅是实现无人飞行管理与控制的关键，而且也是有效载荷信息处理的关键。因此，将可能会采用光学、生物化学、量子力学和分子力学等技术制作处理器，或综合运用上述技术形成某种处理器，进而获得更快的处理速度和更大的存储容量。

#### 3.3 发展系统间的通信技术

美军认为该项技术的核心是数据链和网络中心战通信技术。发展中的通信系统将以网络为中心，许多功能如指挥控制、数据管理和信息流控制等将被集中到作战系统和作战概念中。在数据链技术方面，目前或在今后的一段时期内，无人飞行器需要将全部数据传到地面进行处理并做出决策。随着机载数据链传输速率和处理器运算速度的急速增加，未来的无人飞行器功能将会更加强大。最终，无人

飞行器能够对数据进行本地处理,并将处理后的数据传到地面进行决策;在网络中心战通信技术方面,低速近空间飞行器系统,能够把信息传递到网络中枢并进行网络应用。重点发展以下技术:高容量定向数据链、处理容量大的大型路由器、可编程的模块化路由器体系结构、广泛应用的标准化协议和接口、特设的类似稳态的机动网络、平台网关技术、信息/网络安全技术、性能优越的代理服务器技术等。这些技术带来的网络功能,可使低速近空间飞行器系统平台为部队提供网络中心服务,并且能使低速近空间飞行器系统利用网络扩展功能。

## 4 对临近空间军事开发利用的思考

目前,在临近空间区域主要存在着两个军事应用的空白,一是缺乏持续的通信和情报、监视、侦察效能;二是军事作战武器没有覆盖这一高度。因此,要想在未来战争中立于不败之地,必须要重视对临近空间的开发利用,它是我军建设信息化军队、打赢信息化战争的迫切需要。

### 4.1 加大对临近空间开发利用的理论研究

我国近年来也十分关注对临近空间的开发利用研究。为了研讨临近空间飞行器的关键基础科学问题,探讨发展近空间飞行器的有效途径,国家自然科学基金委员会数理科学部于2006年在北京组织召开了“临近空间飞行器的发展趋势和重大基础科学问题研讨会”。该会对探讨和临近空间飞行器的基础科学问题对临近空间飞行器的发展将起到重要的引领和支撑作用。“空天飞行器的若干重大基础问题”重大研究计划经过前期的努力,进展顺利。

“十一五”期间应加大军事应用理论和技术理论的研究,把握发展机遇,抢夺发展先机。总之,国内外对此研究和开发利用均处于启萌阶段,国内外在该领域理论研究和实践差距不是很大,真正的军事应用还鲜为人见。

参考文献(略)

作者联系方式

通信地址:西安市沣镐路1号训练部装备教保办

邮政编码:710077

联系电话:13363905292

## 4.2 加大对临近空间开发利用的技术研究

随着对临近空间开发利用研究的不断深入,应在我国技术发展情况的支撑下,从临近空间可部署通信设备和情报传感器,以及战斗平台等角度入手,着眼更有效地进行侦察与监视、中继通信、并改进近距空中支援保障,以及设置作战平台等,笔者认为当前应研究以下几个方面的问题:一是未来军事斗争准备对临近空间开发利用的需求;二是临近空间在空天一体作战中的地位和作用;三是当前各国在此领域开发利用的现状与发展;四是技术基础条件和平台应用的可行性;五是对临近空间开发利用的策略及当前急需重点解决的问题等。特别是要重点研究我军对临近空间开发利用的技术基础、目标与途径。如在理论上以军事需求为牵引,提出对发展升空技术、推进技术、材料技术、电源电子技术,以及极小型电子系统的建议。要形成对该空间开发利用的计划和重点项目,发此提升信息化条件下的作战能力。

### 4.3 加大对临近空间开发利用的实践性研究

从有关资料来看,如果某个临近空间平台的飞行高度为36.6千米,那么在零度仰角时其地面覆盖(观测)面积也只是直径为680千米的圆区域,因此,仅适于国土面积较小的国家进行战略侦察任务。采用多层的侦察手段可以使敌方难以实施相应的防范措施,把临近空间平台作为空载和卫星战略侦察能力的强有力的补充,能够承担部分空载平台的战略侦察任务。在战略防御任务中,美军设想将临近空间作为空间效能的备份,它们正在研究在丧失了GPS卫星导航能力的情况下,如何利用临近空间平台进行GPS能力重构替代。从目前的发展状况看,临近空间的军事应用仍处于理论研究和概念验证阶段,但美国正在加快临近空间领域军事应用的步伐,有望在近期部署基于临近空间平台的军用通信系统以及侦察、监视遥感器。

# 浅谈信息作战对炮兵通信的要求

王华命 王生

**摘 要:** 未来信息化作战对炮兵通信提出更高的要求, 本文从炮兵通信分队, 通信技术、通信系统、通信设备、通信保障等方面分析探讨了信息战对炮兵通信的要求, 并结合我军炮兵通信的现状和存在的问题, 提出了一些改进和发展我军炮兵通信的措施和方法。

**关键词:** 炮兵通信; 信息战

信息战是信息技术在军事领域广泛应用的必然产物, 它决定着目前军队建设的重大发展方向。信息战对作战最本质的影响就是它使整个战场信息化、智能化、并使 C<sup>4</sup>I 系统和武器装备的体系、结构和组成发生深刻的变化, 它使传统的通信面临着严峻的挑战。高技术下的现代战场信息量大、电磁环境复杂、目标种类多、停留时间短、战机稍纵即逝, 炮兵作为火力突击的骨干力量, 其火力的强弱, 反应速度的快慢、毁伤能力的大小, 对战役战斗的胜利起着非常重要的作用。炮兵的快速反应能力和火力突然性在很大程度上依赖于其通信系统的性能, 因此, 研究信息作战对炮兵通信的要求与影响, 具有重要的现实意义。信息条件下, 炮兵必须从传统的狭义的单一通信观念转变到广义的通信观念上, 通信不仅仅停留在打通电话、收发提出报文的程度上, 而应该贯穿于信息获取、传递、处理、加工、利用的全过程, 只有这样才能使炮兵通信系统融入整个通信系统中, 在体系与系统对抗中提高自己的抗衡能力。

## 1 信息战对炮兵指挥人员的要求

以知识为基础的信息战要求军队在作战理论、指挥官的培养、士兵训练、编制和装备等方面进行重大的改革, 其中人的因素仍居第一位, 因为指挥人员是否精干高效事关信息战的成败。炮兵通信联络的过程中, 各级指挥员要使用不同的通信设备完成通信联络及协同任务, 各级指挥员使用的通信设备占整个通信设备的 40% 以上。因此, 指挥员是通信联络的“中心”, 指挥员的通信素质与能力对通信网络的稳定性有很大的影响, 炮兵指挥员应精通通信联络组织与指挥。通信指挥的目的是统筹、协

调各战斗通信力量、组织实施战斗通信保障, 确保信息系统的正常、高效运转。信息战中通信保障效能的发挥必将影响战斗指挥的效率, 为了驾驭信息系统, 炮兵部队的指挥员及所属人员必须将各通信设备的技术、战术和作战管理专长融为一体; 必须合理配置和利用各种手段, 达成各作战部队的有效配合。

## 2 信息战对炮兵应用通信技术的要求

信息化作战, 信息系统可能成为兵力倍增器, 也可能成为倍减器, 信息系统的优势并不直接等于战场的优势。也就是说, 单有先进的信息系统不足以成为兵力倍增器, 而必须同时运用保护己方信息系统的保护措施和破坏敌方系统的措施, 即增强通信技术装备的保护能力以及开发对抗能力强的通信技术和新的通信装备。炮兵作为火力支援单位, 其作战完全依赖于各种信息, 因此增强其通信保障能力是必须考虑的。信息战要求通信装备增强防护能力, 提高生存力和安全保密性, 要求炮兵通信系统网络化、数字化, 通信手段多样化, 通信方式简捷化和网络管理智能化, 通信设备小型化和标准化。在通信系统网络化方面, 要开发能够自动重新组网的自由式网络, 以适应作战时网络的迅速变化, 提高通信系统的抗毁性和可靠性, 增强通信网络的互通能力。

通信系统数字化要求把语音、文字、图像等类型的信息进行数字编码, 通过各种信息传输手段, 把指挥所、各作战及后勤分队、各类武器平台乃至单兵都联系起来, 组成一个综合的计算机通信网络, 充分发挥数字通信快速、准确、容量大的优点, 实现上下左右近实时的信息交换。

在通信手段多样化方面,要求综合各种无线电通信手段,增强“动中通”的能力,并能充分利用光缆、电缆等多种有线手段,合理利用通信手段的冗余度来增强通信系统的抗毁能力和反对抗能力。

在网络管理智能化方面,要求进一步提高网络管理的自动化水平,增强网络的灵活性和对付复杂环境的能力。

在通信方式上,信息战对通信装备新的发展需求是视像和多媒体等直观性强的通信方式以及电子邮件、话音信函等快捷简便的通信方式,以增强战略决策和作战指挥的及时性、准确性和有效性。

在通信设备小型化方面,要求通过微电子等技术,降低通信设备的功耗、体积和重量,着重发展便携式、背负式、车载式和机载式设备,增强机动作战能力。

在标准化方面,要求从过去的分立元件向集成模块过渡,增强通信设备的互换性和灵活性,使其操作简单,便于扩展功能,容易维护、开设和撤收、部署和重新部署简便易行,以增强机动战和协同作战的互通能力。为增强通信装备的防护能力,要重点开发利用以下通信技术。

一是开发先进的抗干扰技术。研究和利用扩频、跳频、信号处理(包括卫星信号处理)、天线自适应调零、先进的调制技术(如正交跳频码波形)和时分多址技术等。

二是开发先进的通信保密技术。开发和利用低截获概率/低探测概率的猝发和隐蔽通信技术等。

三是开发先进的多媒体技术,即能自由输入、输出和处理图像、照片、声音、文字、图形、数值等数据的技术,能综合处理大量数据信息,并能相互交换分别管理的信息,从而达到大量、实进、准确地传输信息的要求。

四是反计算机病毒技术,开发抗病毒能力强的软件,增强通信软件抗病毒“感染”能力和防备计算机病毒远程注入能力。

### 3 信息战对通信系统的要求

随着信息战理论研究的深入与实践(含信息高速公路和战场数字化的建设),将对通信联络,包括通信系统、通信设备及通信保障的发展产生深刻的影响,使其呈现下述的各种变化与发展趋势。

#### (1) 综合化

信息战要求炮兵通信系统综合化,使通信系统具有多功能、多手段、高效率、的特点,可实现作战区域内军民各级各类分系统网络兼容,可综合实施指挥协同、报知、预警及其后方通信保障。它具体体现在下述变化。

##### 1) 通信网络综合化。

随着炮兵武器装备、战场环境的全面数字化、单工无线电台通信网、无线电移动通信网、一点多址无线电通信网等通过相应的接口设备,可以在战区C<sup>4</sup>I系统中互通。

##### 2) 通信手段综合化。

无线电接力、无线电移动通信、一点多址无线电、对流层散射、有线电、激光通信等多种通信手段将连成一个有机的整体。

##### 3) 通信终端综合化。

炮兵通信系统的每个用户终端具有多种功能,既能通话,又能发报,还能传输图像。为增强通信指挥和对抗的综合能力,将出现把通信、测向、干扰和自我保护能力以及定位能力集于一体的多功能通信设备,从而增强机动作战能力和战场环境下的快速应变能力。

##### 4) 通信业务综合化。

通信系统可以通过多媒体技术处理电话、电报、传真、数据、图形图像等多种通信业务。

以上四点炮兵通信系统综合化的最根本的目的是利用各种信息基础设施,通过信息战的综合信息控制将炮兵侦察、指挥等不同种类、不同型号、不同用途的武器装备构成一个综合性、纵向和横向互通、能传输多媒体的一体化的整体,以满足未来作战的需要。

#### (2) 兼容性和互通性

信息作战要求各军兵种必须高度重视通信系统的互通性和兼容性,以确保诸军兵种联合作战的协同指挥,以充分发挥各种武器的整体作战能力。通信系统要能够为战场指挥员乃至任何战斗员及时、准确提供其所需的数据。要通过固定式和移动式战术通信中心把各兵种联结起来,实现全网信息共享,力图实现各军兵种C<sup>4</sup>I系统的最大限度的互通。炮兵通信系统要采用标准化的数据传输格式与标准接口,达到各军兵种及友军的互连互通,同时注重提高传输速率,以确保信息设备至信息设备、信息设备至武器系统、传感器至信息设/射手之间

必需的连通性。

### (3) 抗毁性与保密性

为了抵御敌方信息战进攻,炮兵通信系统在结构设置上要有助于抗毁、抗干扰和保密性能的提高。通信系统将采用散射通信、激光通信、数字通信、微波通信等手段。通信系统要采用各种加密手段保障信息的安全,成为有密码保护的、安全可靠的抗干扰通信系统。要配备防计算机病毒的软件和部件,还可通过检查程序来检测暗藏的计算机病毒。

### (4) 立体化

随着信息战理论研究的深入与实践的发展,炮兵通信系统将向立体化配置方向发展。将更多地利用各类空中通信设备。一些通信设备装载在无人机、直升机等平台上,形成立体化配置,以弥补地面通信设备的不足。

## 4 信息战对通信设备的要求

信息战中的炮兵通信设备将变成数字信息技术装备,这些装备将实现如下标准。

### (1) 标准化

在信息战中,对各军兵种联合作战来说,信息的获取、传递、处理、压扩、存储都要求通信设备的软、硬件标准化,如通信协议、功能模块的标准接口设备、加密解密设备等。通信设备将有良好的电磁兼容性,这样既有利于同其他类型的设备、网络和系统接口,又避免了相互干扰,提高了通信设备的互通性和易维护性。

### (2) 模块化

为了提高通信设备的适用性和多功能性,能够根据作战环境和作战任务要求,使其设备组网可大可小,层次可多可少,在结构上采用模块化或模件化,通信设备功能的增强与扩展只是“积木式”的叠加。使一个通信设备通过插拨各种功能卡达到扩展功能和更新换代的目的,实现“即插即用”。这样既提高了设备的通用性和互联性,又使得设备工作方式增多,如发射功率,调制方式变化,工作频段变化等,也使通信、报警、定位、干扰等功能集于一体。

### (3) 小型化

采用了数字技术后,大规模、超大规模集成电路和微处理机得到充分利用,使通信设备向小型化

发展。大大减小了设备的体积、重量及能耗,延长了工作时间。集成电路的使用提高了整机的工作可靠性、稳定性。小型轻便的通信设备便于携带、隐蔽,能适应高速机动作战的要求,提高了机动性。

### (4) 智能化

炮兵联络方向、联络方式的增多,信息的形式多样(图、文、声),设备的多功能化都要求通信设备的自动化与智能化程度要高。比如,电台的自动收、发,接口的自动转接,信道质量检测、自动加密、解密,故障显示及备份启动,真伪识别及自恢复装备的启动,自动实现战斗网之间的横向协调与战斗通信设备的纵向联合,实现军用与民用通信网的转换等等,都需要计算机的辅助,需要智能化和自动化,靠传统的人工操作是不可能完成的。

## 5 信息战对通信保障的要求

信息战的通信装备具有作用距离远、容量大、通信保密性能好、抗毁能力强等优点,不同装备用于不同场合,每类设备都有一定用处。从而保证了战争指挥的高性能、不间断、稳定性和灵活性,也引起了通信保障的深刻变革。随着通信装备的系列化、通用性、数字化、智能化、小型化和模块化,通信将在未来信息战中发挥更为重要的不可替代的作用。从而,使得炮兵通信保障必将达到以下要求。

### (1) 整体化

信息战对战斗通信保障也提出了许多新的更高的要求,特别在整体性上,它集中表现在如下方向。

1) 通信力量编成的整体性。即信息战中的战斗通信力量,是由作战部队通信力量和地方通信力量、民兵通信力量编成的。各种战斗通信力量的有机结合,构成了通信保障力量的统一体。

2) 通信手段运用的整体性。即无线电通信手段、有线电通信手段、运动通信和简易信号通信手段运用结合起来,以便发挥各种通信手段的优点,谋求通信手段的整体优势,发挥通信保障的最佳效能。

3) 通信组织形式的整体性。未来的信息战中,不同的作战样式和战斗的不同时节,将采取不同的通信组织形式和方法,如集中式、地域式、网格式、地域组网与指挥系统组网相结合、多种方式相结合等,并将整体运用。

4) 通信战法运用的整体性。在高技术条件下,根据登陆、山地、城市、等战斗的不同特点和战场的具体情况,炮兵通信将采取“野固并用、车人结合、综合组网、多种手段、整体保障”,“指协一体,移动伴随”,“超越直通,立体覆盖”等战法,并将多种通信战法整体运用。

### (2) 快节奏、多样化、高速化

战场上的通信保障实际上就是实施战斗通信战法。传统的战斗通信战法组织与实施的程序是:先组织计划,再进行战斗通信准备,后按战斗的实施程序进行战斗通信保障。信息战中的各类信息武器装备威力增大,光电杀伤武器的出现及大量使用,在制导、指挥、控制、侦察、通信、电子战等方面广泛应用新的技术,战场侦察、定位、攻击系统的不断发展,加之炮兵自行化、机械化逐步全面实现,使炮兵的反应速度加快,使用时间缩短。战斗通信战法的实施中可能出现逆程序(与常规程序相反),即先集中通信力量,保障战斗主力直接作用于对方纵深,打乱其结构,尔后保障各部(分)队

各个击破敌人,或由后向前攻击。届时,战斗通信保障必须满足快节奏、多样化、高速化的要求。

### (3) 通信组织地域化

在信息战中,炮兵战斗部署将以“大分散”,“高聚能”(集中多种火力打击能量)的形式迅速作用于主要方向和重要目标,高速度、宽正面、大纵深攻击战斗将普遍运用,纵深打击战斗将进一步发展,战斗可能出现违反常规的局面。通信组织的地域化将能满足这些战场需。信息战中,通信组织的地域化,就是在战斗地幅内开设若干个野战干线节点(或通信枢纽)、入口节点、无线电移动通信系统,组成覆盖整个作战地域的公用交换网,在网内诸军兵种移动与固定用户均能互通。它能较好地克服目前战斗通信组织各军兵种的自成体系、按指挥关系组网、通信容量小、抗毁性差、易暴露指挥所位置等弱点,具有组网灵活、迂回路由多、抗毁能力强、便于用户入网、能较好地适应现代战斗的特点。

## 参考文献

- [1] 刘春胜. 联合战役通信学. 北京: 军事谊文出版社, 1999 年
- [2] 建国. 野战综合通信系统. 北京: 通信指挥学院, 2000 年
- [3] 许金裕. 联合战役概要. 北京: 通信指挥学院, 2000 年

## 作者联系方式

通信地址: 炮兵学院南京分院通信教研室

邮政编码: 211132

联系电话: 13814529499

# 战术数据链的综合集成应用

王启国 曲悦

**摘要:**为适应未来信息时代联合作战的需求,美军提出了系统集成的概念,并着力构建 C<sup>4</sup>ISR 体系结构框架。本文在讨论信息系统综合集成的架构和使命任务,分析现役战术数据链的基础上,探讨了战术系统的体系结构和战术数据链一体化的有关问题,并介绍了一种利用军用数据链综合集成(MDLI)应用软件,实现现役数据链平台综合集成的、公共的可升级解决方案。

**关键词:**信息综合集成; 战术数据链

网络中心作战将是信息时代的战争形态。为适应未来联合作战的需求,1997年,美军参谋长联席会议提出了系统集成(System Integration)的概念,同时,美军颁布了《C<sup>4</sup>ISR 体系结构框架》,并先后发布了两版《GIG 体系结构》,以全球信息栅格(GIG)构建新一代一体化的国防信息基础设施,提供以网络为中心的信息环境。

系统集成需要一个综合的架构,以便综合应用信息探测、信息传输、信息处理和指挥决策等各系统的能力,最大限度地提升军队的整体作战能力。系统集成的关键是信息数据集成共享,其基础则是信息数据的传输和交换。本文探讨战术数据链综合集成应用的有关问题。

## 1 信息系统综合集成

信息系统集成的综合架构包括信息保障、指挥控制、部队协同、联合作战体系结构。信息系统综合集成涉及到信息探测层、信息传输层、信息处理层、信息应用层和指挥决策层等诸多层面。信息系统综合集成涵盖了作战体系集成、指控系统与武器系统集成、指挥与信息系统集成、通信系统集成等多项系统集成使命任务。

以美国海军为例,为实现系统集成,计划将指挥与信息基础设施(NCII)作为其网络中心作战的实施架构。该基础设施由实现信息库、传感器、指挥部门、作战部队等单位间的信息交换的通信资源,及允许这些信息用于指挥人员进行决策和指挥的处理计算资源组成。它不仅支持信息的控制管理,而且支持实际的指挥功能。能适应变化的指挥模式,支持所有指挥层次的作战并使之一体化。研

发该基础设施所涉及的业务是一个全面能力的概念。

从系统设计的观点来看,可认为该基础设施包括两个层次:支持性资源基础,和利用支持性资源基础的应用。支持性资源基础的主要功能是提供通信链路,和使之形成网络的通信及组网业务;保证信息的安全;协调资源的使用和带宽的分配并提供端对端业务质量的系统资源管理等。利用支持性资源基础的应用包括信息收集管理,信息的利用与合成,信息请求与分发管理,信息的显示与决策支持,及执行管理等功能;这些专项功能是在支持性资源基础上运行的。

系统应具有在战略和战术层面统一的体系结构。在各层面将应用相同的功能集,与这些功能有关的接口和标准将是相同的,各功能间交换的数据也将尽量使用一致的定义。该架构应具备灵活的、自适应的和可发展的特征。因此,要求支持性资源基础具有必需的容量,连通性和可配置性,互通性和互操作性。

## 2 战术系统的体系结构

该架构以适当的层次结构来支持各指挥层次的作战,并使之一体化。系统应包括三层网络:联合计划网(JPN),联合数据网(JDN)及联合合成跟踪网(JCTN)。联合计划网应用于战略层面,联合数据网及联合合成跟踪网属战术层次,是两类专用的战术无线电网络。

联合数据网是基于各种战术数字信息链(TADIL)、公共数据链(CDL)和战术信息广播业务(TIBS)等战术数据链构成的数据网络。



公共数据链(CDL)属于相对通用的宽带战术数据链,是一个全双工、抗干扰、点对点的微波通信系统。它可以从空中平台发送雷达、图像、视频和其他传感器信息,并将控制数据传给空中平台。公共数据链系统是指一系列可互操作的数据链路,可装载不同的平台,并可通过多种方式进行扩充和配置,具有宽带、大容量的特点。另外,工作在Ku波段的战术公共数据链(TCDL),适于装载战术无人机。

已经并入综合广播业务(IBS)系统的战术信息广播业务(TIBS),利用飞机或UHF卫星通过保密的通信广播,向各作战单元提供近实时的、多传感器获取的、多源的位置态势和威胁告警信息,其中重点是分发有关跟踪精度的信息,可采用动态时分多址(TDMA)方式组网工作,使用类似TADIL J的报文格式,并允许在网络参与者间进行交互式信息交换。具有较大的容量、较好的互通性和互操作性。

TADIL J(Link 16)是美军用于C<sup>4</sup>I系统的主要战术数据链,可以构成一种大容量、保密、抗干扰的数据链路,支持监视数据、电子战数据、战斗任务、武器分配和控制数据的交换,工作在Lx波段,采用时分多址(TDMA)方式组网,使用J系列报文,并遵循联合战术信息分发系统(JTIDS)/多功能信息分发系统(MIDS)的通信标准。配备有适于装载不同平台的各类端机,具有很好的可配置性。

TADIL A(Link 11A)是用于舰艇编队的数据链路,在岸基、机载和舰载指挥控制系统间交换战术数据。工作在HF和UHF频段,在网络控制站的控制下,以轮询(ROLL CALL)方式工作,也可通过广播方式发送信息,采用M系列报文。Link 11的改进型TADIL F(Link 22)综合了Link 11和Link 16的功能和特点,使用F系列报文,采用时分多址(TDMA)体系结构,信息传输速率高于Link 11,具有很强的可配置性、互通性和互操作性。

公共数据链和信息广播业务的某些应用,传输的数据能达到目标精度,传输时延为毫秒级,可用作武器控制级数据链,能与协同作战能力(CEC)等战术链路构成联合合成跟踪网。

系统集成需要在各层次间具有相同的体系结构。目前,在战略层面,基于因特网的协议被广泛

地应用;而战术网络还是一些专用的无线网络。美军考虑利用商业技术与军用技术混合的方式来增强用于联合数据网的战术网络。而直接用于对武器控制,支持武器协同的联合合成跟踪网要求极短的传输延迟,且武器控制过程不需指挥员直接介入,故暂不强求改变其专用的网络协议,但其接口必须满足系统设计中建立的标准。

集成战术数据链的基本原则应该是在一体化设计的基础上,注意在战术部分和非战术部分的连接点处设置严格的控制,确保只有经过授权的业务才允许进入战术网,保证战术网能提供高可靠、低等待的数据业务。

### 3 战术数据链的一体化

为了便于信息系统集成和构建一体化的C<sup>4</sup>ISR系统,美国国防部正在开发用作标准数据链电台的联合战术无线电系统(JTRS),并选择J系列报文作为战术数据链的消息标准。JTRS已涵盖了Link 16的波形。未来的军事平台将使用该系统实现战术数据链的能力。美国国防部计划到2015年以后,大量现役的各种传统军事平台将被一体化的JTRS更新换代。

另外,北约研发的TADIL F(Link 22)使用由J系列报文衍生出的F系列报文,采用时分多址(TDMA)体系结构,综合了Link 11和Link 16的功能和特点。配备Link 22的单元被称为NILE(NU),能够通过数据转发单元(FNU)与配备其他战术数据链(如Link 16及Link 11/11 B等)的单元交换战术数据,实现消息的转发和战术信息的综合。

Link 22数据链终端NILE(NU)由数据链处理器(DLP)、系统网络控制器(SNC)、链路层通信安全(LLCS)模块、信号处理控制器(SPC)及HF和UHF电台构成。Link 22数据链系统的基本结构如图1所示。

其中,RADIO为定频/跳频HF/UHF电台;信号处理控制器(SPC)完成调制解调和检错纠错;链路层通信安全(LLCS)模块利用时间和用户地址编码提供网络的安全保障;系统网络控制器(SNC)提供报文传输,以及网络和管理服务,实现动态TDMA协议、控制中转、路由、迟入网和流控;数据链处理器(DLP)实现与系统网

络控制器（SNC）接口，提供必要的显示服务，生成和转发报文，完成消息数据的格式转换、消息转发和按优先级排序等功能，并与战术数据系统（TDS）接口，接受 TDS 请求发送的数据，将从

链路上接收到的数据馈至 TDS。战术数据系统（TDS）是通过 Link 22 数据链传输的报文的信源和信宿。

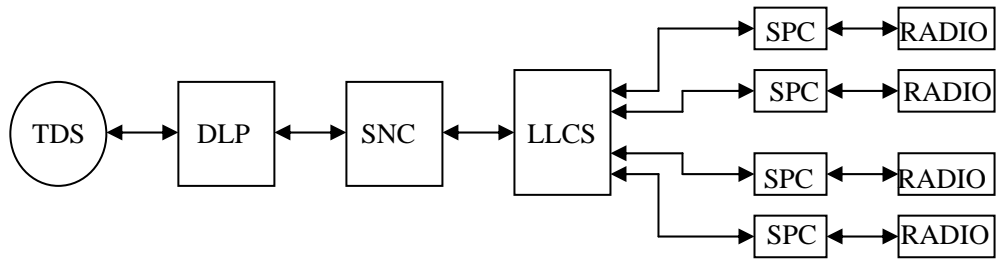


图 1 Link 22 数据链系统的基本结构

其关键部件数据链处理器（DLP）不仅与战术数据系统（TDS）接口，而且和其他的战术数据链接口，实现不同战术数据链间的数据转发，应用于战术信息的综合。

4 数据链平台综合集成

据统计美军已经有近 28000 个数据链平台，从进度和经费上来说都不可能在短期内完成全面更新的任务。为了能继续利用数据链平台现有的资源，同时能与新的系统接口，美国等北约国家军方正在探讨多种公共的可升级的解决方案，如联合战术体系结构（JTA），软件通信体系结构（SCA），军用数据链集成（MDLI）应用软件等。

军用数据链集成（MDLI）应用软件是一种利用计算机完成软件处理和维护，实现数据链平台综合集成的解决方案。其组成包括：数据链消息处理、数据链平台综合、主机平台结构数据库、消息参数数据库和用户可更改（UMI）数据库等。主机计算机系统由应用处理器模块、图像处理模块及 I/O 模块组成。运行的预定义数据交换协议由主计算机系统口地址、消息结构和格式、数据交换命令系列组成。

MDLI 应用允许各独立的数据链平台重构实现其能力的数据库，及共用该平台各子系统的接口指令，能实现特殊的消息处理功能。这些功能包括对来自完全不同的信息源的数据相关，目标轨迹队列，数据格式化，自动激活和关联行动，自动触发报文发送，任务记录及回放，以及提供数据链显示格式和视频输出等。

MDLI 应用软件的解决方案，可按需要应用于

任何消息标准或标准集。以使用 Link 16 战术数据链的报文标准，即 J 系列消息为例，采用该方案完成数据链平台综合集成的技术实现见图 2。

数据链消息处理软件，首先利用在主机平台通信设备结构数据库中预定义的指令，初始化建立与通信分系统的接口。该数据库提供主机应用处理器为各可用通信分系统设定的端口地址和协议，消息结构和格式，及完成数据交换的命令系列。初始化后，按预定的速率、消息处理标准和网络管理规则，输入的消息被译码，输出的消息被编码。从输入消息中获取的消息参数存入消息参数数据库。特定的消息功能基于用户可更改数据库的指令来实现。

数据链平台综合集成软件，首先利用在主机平台显示设备结构数据库和任务设备结构数据库中预定义的指令，初始化建立与传统子系统的接口。这些数据库将指示有那些子系统是可以利用的，并提供为了与每个可用的传统子系统交换数据的主机应用处理器端口地址和协议、消息结构和格式、命令系列等。初始化完成后，来自子系统的输入数据被译码，输出到子系统去的消息参数数据库中的数据，将按平台的要求格式化，再编码成适当的消息格式发送到相应的子系统。特定的平台功能基于用户可更改数据库的指令来实现。

用户可更改数据库的指令功能包括：数据收集指令用来识别从主机平台上的子系统收集的数据参数，并存入消息参数数据库；消息处理指令用于激活用户指定的数据处理，如数据融合运算，创建和更新轨迹队列，创建和更新已知的态势共享信息等，相应的结果存入消息参数数据库；路由指令用于确定将消息参数数据库中数据发送到特定的子系

统或通信分系统；显示格式指令用于选择数据的显示格式。

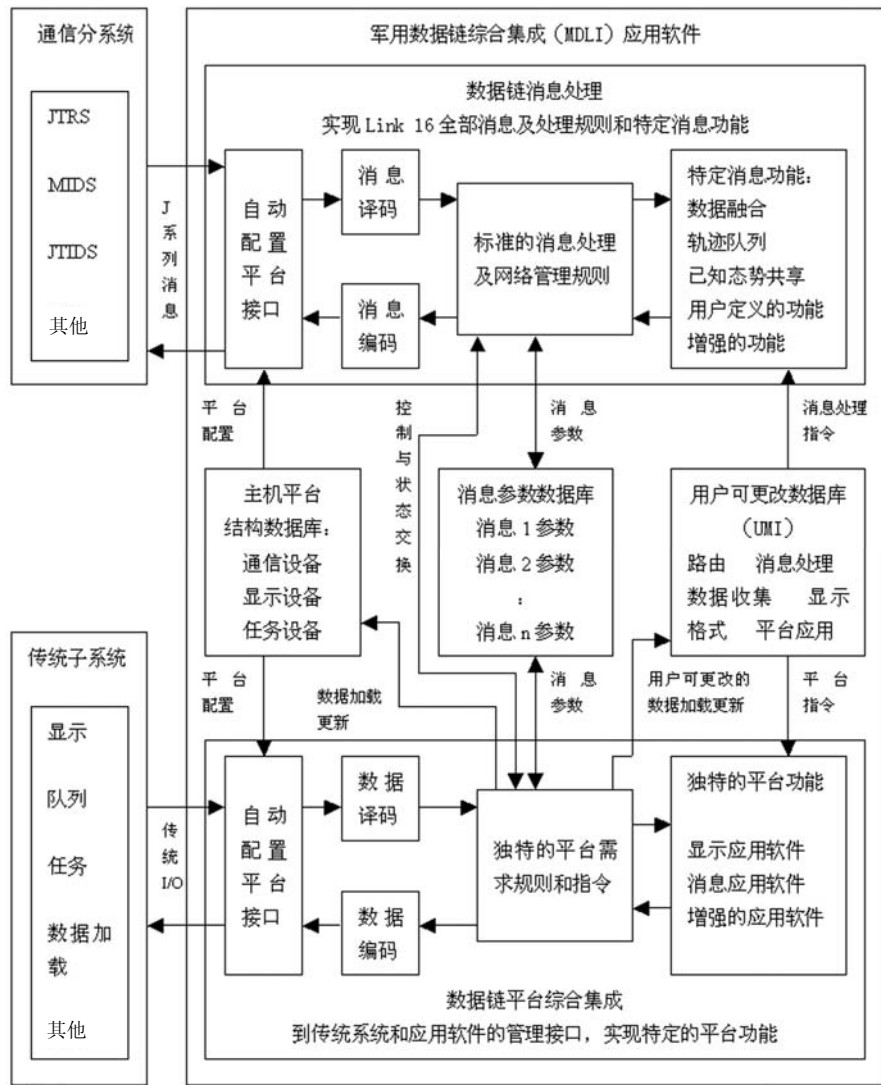


图2 数据链平台综合集成的技术实现

针对具体的数据链平台，MDLI 应用软件可以基于专用的主机运行，也可以寄生于该平台传统设备备的图像处理模块（IPM）或通用处理器（GPP）中运行。从而实现数据链平台的综合集成。

## 参考文献

- [1] James T. Sturdy “Military Data Link Integration Application”

## 作者联系方式

通信地址：武汉市 70005 信箱

邮政编码：430079

联系电话：027-67889524

# 数据资源共享中的交换机制研究

胥少卿 罗强一 刘新盛 景柏树

**摘 要：**本文结合数据共享中的交换方法研究现状，针对数据交换的核心问题—异构本体交换，构建了基于交换中心的数据交换平台框架，讨论了基于本体的数据表示方法，对当前异构本体映射方法进行了分析比较。

**关键词：**共享；数据交换；本体；映射

数据资源共享是信息系统集成的一个重要组成部分，而共享能力不足已经成为影响信息系统建设的瓶颈。数据交换能力作为共享服务的一个重要方面，能够在根本上提高数据共享水平，因此也是研究和发展的重点。

## 1 数据交换与数据资源共享体系

数据交换与数据共享密不可分，数据共享的主要目的是为用户提供一种透明访问异构数据源的方式，使各数据源的数据对用户可见、可用。制约数

据共享的一个主要原因是海量数据资源的异构性，数据交换的作用在于从语义的层次来完成异构数据的理解和交换，保障综合系统中各子系统和数据源中的异构数据相互转换，使数据共享成为可能。

数据资源共享服务平台依托各业务数据库、共享数据库等数据资源和数据定义标准，通过元数据与资源目录的注册管理、数据交换服务等功能完成数据共享。其总体架构包括元数据与目录注册管理模块、数据交换平台、共享平台管理模块和各应用子系统 4 大部分，具体如图 1 所示。

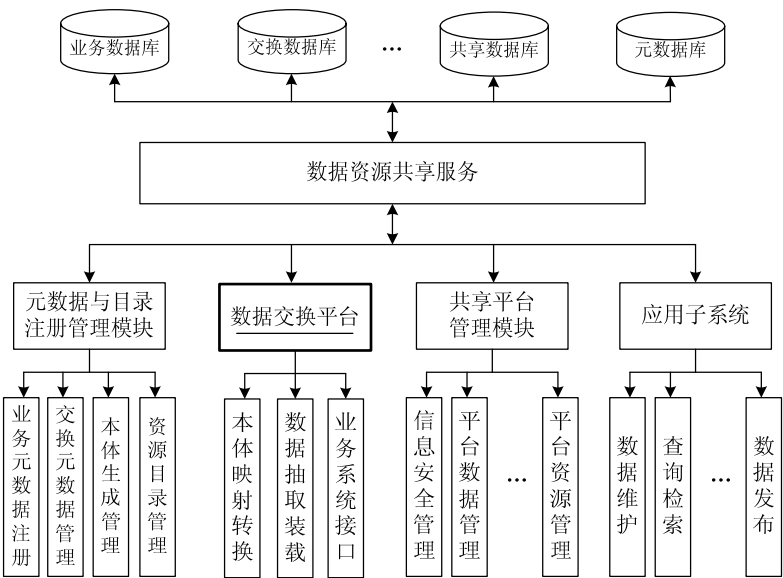


图 1 数据资源共享服务体系的总体架构

其中的数据交换平台是数据资源共享体系中的一个关键模块，不同模式、不同来源的业务数据通过本体进行定义，在数据交换平台完成转换，为数据的有效共享奠定基础。

一个完善的数据交换平台需要解决的首要问题

是数据的异构问题。数据资源的异构可分为数据异构（data heterogeneity）和语义异构（semantic heterogeneity）。一般说来，解决数据异构问题需要在数据语义明确的前提下采取消除冲突的方法，相对来说较容易。为了抓住关键环节，下文中所涉

及到数据交换的内容和方法都侧重于解决语义异构问题。此类问题的解决方法最终都要归于数据交换模式的良性构建和数据语义的严格定义与映射上。

## 2 基于交换中心的数据交换模式

通常的数据交换模式有两种，一是点对点交换，二是基于交换中心的系统架构方式<sup>[11]</sup>。前者的缺点是连接数随交换点个数呈几何基数级增长，维护工作量较大。后者的连接数呈线性增长，支持点对点 and 订阅/发布式数据交换，便于维护。本文采

取第二种模式，并对其进行扩展。

### 2.1 交换模式的架构

文中提出的交换模式以异构本体的映射匹配作为交换功能的核心算法，架构主体包括数据交换中心与数据交换端节点两大模块。通过建立统一的数据交换中心，将数据交换的重心放在中心处理组件上，数据交换端节点完成各业务系统数据的抽取和加载，并处理其数据交换请求和应答。其概念架构如图2所示。

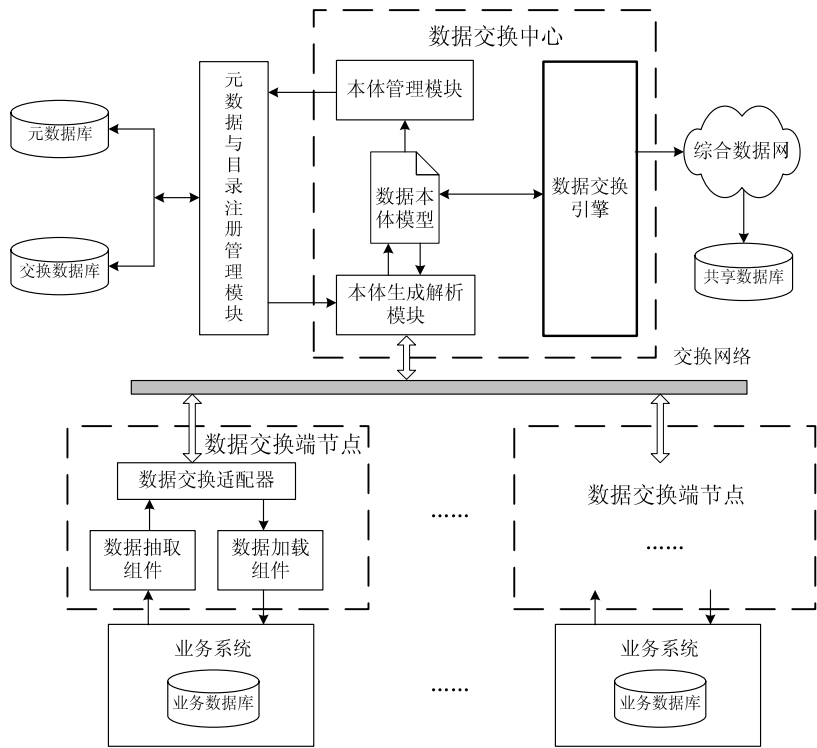


图2 基于交换中心的数据交换模式概念架构

在面向数据共享的交换模式架构中，要借助共享平台的元数据注册管理模块与数据交换中心交互，完成数据本体的生成和注册管理。共享平台中的元数据库、交换数据库、共享数据库等存储载体也为数据交换提供数据资源和交换标准。

### 2.2 主要模块工作机制

数据交换中心是交换平台的关键组件，包括了本体生成解析模块、数据交换引擎和本体管理模块三个主要部分共同完成基于本体的异构数据交换。其工作机制为：本体生成解析模块从交换网络中获取某一个端节点发送的数据信息，从元数据注册管

理模块中调用源端与目的端的元数据表示标准和本体定义模式，生成数据本体模型，将其传送到数据交换引擎，通过本体映射算法将其转换为与目的端数据格式相同的本体模型，再通过本体生成解析模块将其解析，发送给目的端节点。交换引擎同时与共享数据库相连，查询本体映射时的关联信息。本体管理模块对转换前后的异构本体进行登记入库或删除。

数据交换端节点主要完成与各业务系统和业务数据库的连接和数据传输，是交换平台的辅助组件。其工作机制为：数据抽取和加载模块与业务系统相连，从业务数据库中抽取和加载数据。数据交

换适配器通过系统管理、数据压缩、加密、数据交换路由解析、断点续传等技术保证各系统之间和端节点与交换中心之间安全、准确的数据交换。一方面,数据交换适配器将抽取的数据提交给数据交换中心,另一方面,各业务系统通过它接收从数据交换中心分发过来的数据,存入相应的业务数据库中。

### 3 基于本体的语义信息模型及交换方法

基于本体的数据交换算法是保证数据交换有效完成的关键,数据交换中心的核心模块都以数据的本体模型为主要处理对象。本节将结合当前研究现状,对基于本体的语义信息模型及其映射方法进行阐述。

#### 3.1 基于本体的数据表示方法

本体是对客观存在的系统的解释或说明,是解决语义层次上信息共享和交换的基础。Gruber<sup>[1]</sup>给出了本体的最为流行的定义,即“本体是概念模型

的明确的规范说明”。通常本体的表示方法有两种:形式化定义和基于本体语言 OWL 的表述。

其形式化定义为  $O = \{C, AC, R, AR, H, X\}$  代表一个本体,其中  $C$  是该本体的概念集合。 $AC$  是多个属性集合组成的集合,其中每个属性对应于  $C$  中的一个概念。 $R$  是本体的关系集合, $AR$  是多个属性集合组成的集合,其中每个属性对应于  $R$  中的一个关系。 $H$  表示概念之间的层次结构关系。 $X$  表示公理集合。例如,由表 1 建立的 *Student* 关系数据模型,其形式化定义为:

$$\begin{aligned} TStu &= \{sStuNum, sCourse, nGrad, sDep\}, \\ Equivalent(sStudentNum, TCourse, sStuNum, TStu), \\ Equivalent(sCourse, TCourse, sClass, TStu), \\ Equivalent(nGrade, TCourse, nGrad, TStu), \\ Equivalent(sDept, TCourse, sDep, TStu) \end{aligned}$$

本体表示数据信息时还可以由 OWL 来描述。OWL 是一种定义和实例化“Web 本体”的语言,是 W3C 目前描述本体的最新标准语言,旨在用于那些需要由应用程序而不是由人来处理文档中信息的情形,适于将异构数据表示成本体的形式,并由交换中心自动或半自动的完成数据的交换。图 3 显示了表 1 建立的数据模型对应的 OWL 代码片断:

```
<owl:Class rdf:ID="TStu"/>
<owl:DatatypeProperty rdf:ID="sDepartment"/>
<owl:equivalentProperty>
  <owl:equivalentProperty>
    <owl:DatatypeProperty rdf:ID="sDep"/>
  </owl:equivalentProperty>
  <rdfs:range rdf:sresource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:equivalentProperty>
.....
```

图 3 Student 的 OWL 代码片断

表 1 Student 关系表

TStu	
sStuNum	String
sCourse	String
nGrad	Int
sDep	String

关联,通过语义的联系,实现将源本体的实体(概念、实例、属性等)映射到目标本体实体上的过程<sup>[6]</sup>。映射的分类按照不同的标准有所不同,可基于语义、概念实例、概念定义和概念结构对本体映射方法进行不同的分类<sup>[8]</sup>。按照文献[2,5,10]中的分类方法,根据本体映射中最重要的一环一本体匹配的不同手段对本体映射分类如图 4 所示。

#### 3.2 本体映射方法的分类

本体映射是指在两个本体中存在语义级的概念

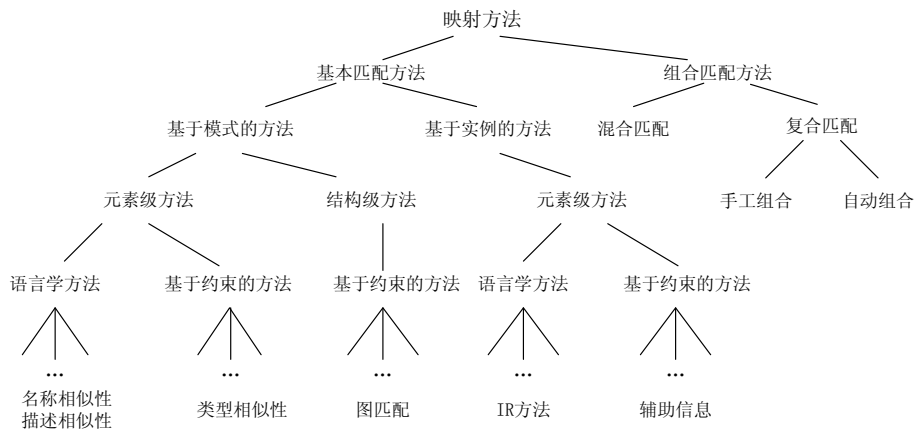


图 4 本体映射分类

各种方法的匹配原则为：

模式级与实例级：前者只考虑本体的模式信息，而不考虑本体的实例数据；而后者综合利用了两者的信息。

元素粒度与结构粒度：前者只考虑本体中独立的概念元素，后者还考虑这些概念元素的组合。

基于语言与基于约束：前者根据本体中元素的名称和描述文本进行匹配，后者根据基本的约束信息。

3.3 本体映射算法的比较

本体映射匹配方面的算法研究已有较多的成果，其中较为典型的有 GLUE、AnchorPROMPT、QOM、Cupid 等<sup>[2,3,4,7,9]</sup>。接下来将按照前文中的分类方法，对这些算法进行分析比较。

GLUE 系统主要是面向实例的匹配，用机器学习

习的方法来完成不同本体间的匹配任务，其思想是多策略学习。它代表了一种自动合并不同匹配器匹配结果的组合方法。

AnchorPROMPT 是基于结构的本体映射发现技术中的一项典型工作，它以基于术语技术得到的本体映射结果为基础，进一步分析本体图的结构相似性，从而发现更多的本体映射。

QOM 是采用综合方法发现本体映射的典型范例。在寻找映射的过程中同时考虑了映射结果的质量与发现映射的时间复杂度，力求寻找二者的平衡。

Cupid 是一种基于元素级匹配和结构匹配的混合方法。它可用于数据库，本体库等多种领域的匹配任务。其思想是：如果两个概念的子概念是相似的，那么它们也趋向相似。

表 2 本体映射算法的比较

		GLUE	AnchorPROMPT	QOM	Cupid
匹配粒度		元素级和结构级	元素级和结构级	元素级和结构级	元素级和结构级
方法分类	基于名称	名称，同义关系	名称，术语对，有向图对应	名称，标识，原语，领域特征，同义关系	名称，同义关系，上下文关系，多义关系
	基于约束			数据类型	数据类型
	结构匹配		路径匹配	叶节点	叶节点子树匹配
	实例级	贝叶斯分类器			
	重用信息	比较训练实例，查询有效领域值	概念间的相似度分数	词典,最大邻近匹配相似度，相似度阈值	词典，词汇表
匹配器组合方式		机器学习方法自动组合		综合	混合
用户交互		可添加匹配和失配规则，人机交互优化结果	可通过用户的直观经验进行相似度分数调整	可调整时间复杂度和结果质量的权重系数	可调加权系数

上述这些本体映射的方案在以下几方面还有待提高：一是对不同领域的本体间结构的差异性考虑不足，同一个映射解决方案对不同应用领域表现出不同的性能；二是大多数方案都是从本体映射的准确性方面进行研究，无法照顾到计算效率和计算成本方面的需要；三是匹配方法缺乏通用性，导致映射过程的模块化程度不高，开放性和普适性较差。

## 4 小结

本文对数据资源共享中的数据交换问题展开了研究探讨，分析了数据交换平台在共享体系中的作用，并针对语义异构问题，构建了基于交换中心的数据交换平台框架。在对当前异构本体映射算法的分析比较中，提出了经典算法的不足之处，对数据交换方法的改进有借鉴意义。

## 参考文献

- [1] Gruber T R. A Translation Approach to Portable Ontology Specifications. Knowledge Acquisition, 1993, 5: 199 - 220.
- [2] Do H.H., Erhard. COMA-A System for Flexible Combination of Schema Matching Approaches. In: Proc. of the World Wide Web Conf., 2002: 85-90.
- [3] Madhavan J, Bernstein P.A, Rahm E. Generic schema matching with cupid. In: Proc. of the 27th Intl. Conf. on very Large Databases, 2001: 49-58.
- [4] Ehrig M, Staab S. QOM-Quick Ontology Mapping[C]// In: ISWC 2004, LNCS 3298, 2004: 683 - 697.
- [5] Melnik S, Garcia-Molina H, Rahm E. Similarity Flooding Versatile Graph Matching Algorithm In Proc. of the 18th Intl. Conf. on Data Engineering (ICDE). San Jose. CA. 2002: 331-336.
- [6] Dian A, Madhavan J, Domingos P., Halevy A. Learning to map between ontologies on the semantic web. In Proc. of the World-Wide Web Conf. (WWW-2002), 2002: 243-248.
- [7] 付相君. 基于本体和 Semantic Web 技术的产品知识集成基础研究. 浙江大学学位论文. 2005.6.
- [8] 徐宝文, 陆建江. 语义 Web 与本体论技术. 南京大学出版社. 2005.8.
- [9] 郑晓峰, 高景昌, 朴忠淑. 基于 Web Service 的语义匹配模型. 吉林大学学报(信息科学版). 2005.9: 552-558.
- [10] 袁洋, 李善平. 基于语义 web 的本体映射方法综述. 计算机科学. 2004.5: 5-8.
- [11] 马忠贵, 叶斌, 王宗杰, 王成耀, 涂序彦. 数字气田中数据交换中心的研究与实现. 计算机工程与设计. 2006.8: 2921-2924.

## 作者联系方式

通信地址：北京市丰台区大成路 13 号 R00

邮政编码：100039

联系电话：010-66820297



# 基于关联矩阵的C<sup>4</sup>ISR系统作战体系结构建模研究

徐佳 顾健 张祥林

**摘 要:** 本文从 C<sup>4</sup>ISR 系统作战体系结构研究的必要性入手, 介绍了作战体系结构及其相关产品, 指出了现有 C<sup>4</sup>ISR 系统作战体系结构缺少作战节点和作战活动关联关系的定性描述。在此基础上, 针对作战节点和作战活动之间的关联关系, 利用作战节点连接图和作战活动模型之间的联系, 建立了关联矩阵, 进行了编程设计, 为 C<sup>4</sup>ISR 系统体系结构的设计提供了技术支持。

**关键词:** C<sup>4</sup>ISR; 作战体系结构; 体系结构产品; 作战节点; 作战活动

## 1 引言

高技术条件下的现代战场情况变化捉摸不定, 频繁的攻防转换、远程空袭、夜战、导弹战、精确打击、电子战、立体战、大纵深战等等, 都给战场设置了众多的未知因素, 使得现代战争具有大纵深、立体化、速决性等特点。在这样的作战环境下, 指挥员需要在极短的时间内综合考虑, 制定对策下达作战任务, 依靠人工作业是不可想象的。可见, C<sup>4</sup>ISR 系统在战争中的地位和作用越来越明显。正如美国国防部就海湾战争向国会提出的那样: “没有可靠的 C<sup>4</sup>ISR 系统, 最好的人员, 最好的设备, 最好的计划都没有多大价值”。为适应战争的需要, 各国都很重视 C<sup>4</sup>ISR 系统的研究, 在 C<sup>4</sup>ISR 系统研发过程中, 通过建立作战体系结构, 来描述作战所需要的每种信息交换的特性, 进行具体的需求分析, 保障所开发的 C<sup>4</sup>ISR 系统满足军事需求。作战体系结构的建立是研发 C<sup>4</sup>ISR 系统的关键环节, 加强作战体系结构的研究, 以保证最终的系统具有较强的针对性和实用性, 真正能为提高我军作战能力做出贡献。

## 2 作战体系结构及其产品

作战体系结构是任务和行动、作战要素以及完成或支援军事作战要求的信息流的一种描述。作战体系结构以任务领域或以作战过程为基础, 确定作战人员的信息需求, 表述 C<sup>4</sup>ISR 系统支持的作战职

能和逻辑要求, 定义信息类型、交换的频段以及由这些信息交换所支撑的任务。

体系结构产品是指在构建一个特定体系结构过程中, 所开发的图形、文字和表格等文档或数据库。它描述了构成体系结构的目的、用途和与其相关的特性等。与作战体系结构相关的标准产品侧重于 C<sup>4</sup>ISR 支撑的作战上下关系, 所支撑的使命和任务, 为执行任务涉及的作战要素, 为满足作战需要所必需的信息交换等方面。作战体系结构产品包括: 高级作战概念图 (OV-1), 作战节点连接图 (OV-2), 作战信息交换矩阵 (OV-3), 组织关系图 (OV-4), 作战活动模型图 (OV-5), 作战规则模型 (OV-6A), 作战状态转换描述图 (OV-6B), 作战事件/跟踪描述图 (OV-6C), 逻辑数据模型图 (OV-7)。

本文关联矩阵的设计实现工作与作战节点连接图 (OV-2) 和作战活动模型图 (OV-5) 有关, 因此重点选取 OV-2 和 OV-5 进行介绍。

作战节点连接图 (OV-2): 表示为完成活动所需节点, 活动和联系的直观图示。这种图的主要特点是描述节点、节点之间的连接以及所交换信息的特征。

作战活动模型图 (OV-5): 描述了支撑某个特定使命所必需执行的特别的作战任务有关的可实现的有关活动, 以及活动之间的关系, 活动之间交换的数据或信息, 以及与该模型范围之外的其他活动所交换的数据或信息。它的特点是对作战活动进行联结, 根据体系结构的等级将活动分配到各节点。

### 3 关联矩阵的建立

#### 3.1 关联关系描述

体系结构产品之间存在逻辑关系，不同产品的数据元素之间也存在联系，如：高级作战概念图 OV-1 的组织、设施与作战节点连接描述图 OV-2 中的作战节点映射，OV-1 中的关系与 OV-2 的需求线对应，OV-2 的需求线又与系统体系结构中系统接口描述图 SV-1 中的一个或多个接口对应，OV-2 中的节点与 OV-5 中的活动相关联。因此，每个产品业务功能处理模块在设计上不是相互独立的，内部数据存在关联关系。

有效利用关联关系可辅助系统顶层设计。例如在充分了解节点和活动的关联信息后，可分析研究所需的系统能力，用来决策需要什么样的系统来满足某个组织或功能领域的作战需求，对于系统体系结构 SV 的功能和物理实现的设计具有辅助作用。

作战体系结构产品中作战节点连接图 OV-2 实际上是作战活动模型 OV-5 的由里及表，其节点对应的各自完成的活动可能是一个或者多个，在 OV-2 的图中特别是复杂系统节点对应大量活动时无法将节点对应的活动罗列在节点边，这样也是不科学的表现方式。同样在作战活动模型 OV-5 中，模型具有层次结构性，即它的开始都是以一个单框来表示最顶层整体活动，然后逐次进行分解，一直到体系结构目的所要求的层次为止。各种活动对应着相应的节点，顶层活动和细化的下层或底层活动可能由同一个节点完成，同一层活动模型中，一个活动可能对应多个节点，多个活动也可能对应一个节点，这样，在活动模型中也无法有效的将对应节点表现出来。因此，建立活动与节点之间的关联矩阵对于建立作战体系结构和分析系统功能具有重要的作用和意义。

#### 3.2 关联矩阵的设计与实现

在现有的作战体系结构产品中并没有节点与活动之间的关联矩阵，因此本文利用 Popkin Software 公司的 System Architect (SA) 软件进行节点与活动关联矩阵的编程设计，根据 OV-2 的节点和 OV-5 的活动之间的关联关系自动生成关联矩阵。在此关联矩阵中，矩阵行是活动，列是节点，在矩阵的方格中通过打 X 来表示对应的节点和活动具有关联

关系，并且在相应方格中可以加入文字，以注释关联关系的具体信息。

从 SA 软件中可导出 USRPROPS.TXT 文件，在此文件中可编写代码以生成矩阵。

本文所实现的 OV-2 和 OV-5 活动与节点之间的关联矩阵代码如下：

```
REM "====Operational Node to Operational
Activity Matrix Cell (可注解矩阵)===="

Rename Definition "User 6" To "Node/Activity"
DEFINITION "Node/Activity"
{
  ADDRESSABLE
  LAYOUT{COLS 2 TAB ALIGN LABEL}
  PROPERTY "Impact Statement" { EDIT Text
LENGTH 1000 }
  PROPERTY "RowDefinition"
  {KEY EDIT OneOf "Operational Activity"
RELATE BY "is part of"}
  PROPERTY "ColumnDefinition"
  {KEY EDIT OneOf "Operational Node" RELATE
BY "is part of"}
  PROPERTY "Description"
  {EDIT Text LENGTH 255 HELP "Appears in the
cell of a matrix"}

  PROPERTY "Intersection?"
  {EDIT Boolean LENGTH 1}
}
```

在代码编写完成后，导入 USRPROPS.TXT 文件，并如图 1 所示。

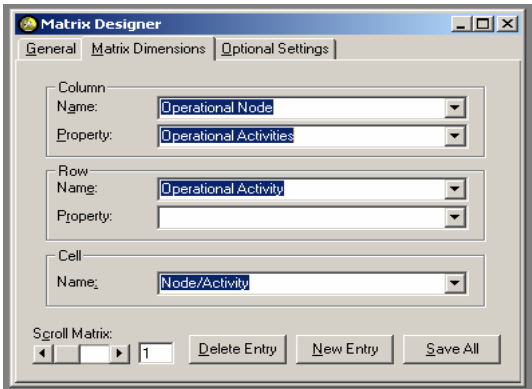


图 1

在 SA 软件的“矩阵编辑”功能中新建矩阵，在“General”中输入矩阵名称，行和列分别选择所

编代码中的"Operational Node"和"Operational Activity",确定以后可自动建立关联,生成矩阵。在用户框中可查阅矩阵,并根据作战体系结构的建模需求加入文字的注释。

### 3.3 关联矩阵的应用

#### (1) 易于系统分析

通常 C<sup>4</sup>ISR 系统是一个复杂的系统工程,系统的功能覆盖面广,涉及的部门多,系统集成工作复杂,若不建立关联矩阵,而在分层显示的作战节点连接图和作战活动模型图中,把各节点进行的活动和各活动所需的节点分别罗列出来,则会使原本已经复杂的模型图变得更加臃肿,并且罗列的节点和活动重复冗余的居多,这样不仅对模型的美观和建立不利,还易造成需求和系统功能分析上的失误及不该有的遗漏,因此,建立节点和活动的关联矩阵,使得关联关系直观明了,可助于科学有效的分析作战需求和系统功能,为系统体系结构的设计提供有效的帮助和参考;

#### (2) 利于模型改进

建立关联矩阵后,可判断分析各节点是否有相关的活动和功能体现,各活动是否有相关的系统或组织来支撑,从而进一步细化系统的任务和使命要求,确定任务执行部门的结构组成、指挥关系,梳理各业务活动的组成及其之间的信息交互关系等内容,删减冗余或增加缺少的节点,对活动模型的分层和流程细化进行优化,使模型设计更加贴近实际

符合 C<sup>4</sup>ISR 系统设计需求;

#### (3) 辅助设计系统体系结构

通过节点—活动矩阵明确了系统中节点与活动之间的相互关系后,结合作战需求可分析系统应具备的能力,在设计系统体系结构时,可根据作战节点的组成、需要完成的作战活动和系统能力,明确系统功能对节点的分配关系和节点的物理实现,从而为系统体系结构的设计提供更科学有效的参考。

## 4 结束语

在体系结构开发过程中,标准模块是基础,其中“通用联合任务表”严格命名和定义了相关的术语,可在联合作战指挥官、参谋人员和系统分析开发人员之间建立一种通用语言和参考系统,以利于作战体系结构的建立。但美军的“通用联合任务表”只能作为参考,必须根据我军的特点和实际,确定我军自己的标准模块,从而有助于作战概念、互操作能力以及系统相关问题的理解,加速我军 C<sup>4</sup>ISR 系统的研制进程。

本文描述了作战节点连接图和作战活动模型图的节点和活动之间的关联关系,利用 SA 软件的编程设计功能自动建立节点活动关联矩阵,并阐述了建立此关联矩阵的优点,为作战节点连接图和作战活动模型图的设计改进提供了帮助,更为系统体系结构的设计提供了科学有效的参考。

## 参考文献

- [1] 黄兆坤 李民. 国外 C<sup>4</sup>ISR 的发展现状与发展趋势. 中国电子学会电子系统工程分会第九届 C4I 理论学术研讨会论文集: 20-24.
- [2] 电子科学研究院系统工程总体部编译. C<sup>4</sup>ISR 体系结构框架(1.0 版本). 1997.

## 作者联系方式

通信地址: 北京市海淀区万寿路 3 号院 91655 部队

邮政编码: 100036

联系电话: 010-66974132

# 导弹保障装备测试信息集成系统开发研究

于光辉 徐明 高山 任海峰 童书辉

**摘 要:** 分析了部队导弹保障装备的特点,说明了测试数据管理的紧迫性,介绍了系统的开发结构和使用的平台和关键技术,得出了可以通过本系统能够将测试数据信息有效管理起来和进行应用的结论。

**关键词:** 测试信息; 数据库; 导弹

## 1 前言

由于导弹种类繁多,检测原理各异,测试设备的开发生产单位也不尽相同,导致各种导弹测试设备的测试数据结果的存储也各异。查看测试数据的结果只能利用测试设备自带的软件打开或由自带软件打印后上报,使得这一过程脱离不开测试设备;每台测试设备的测试数据只能存储在本测试设备的存储介质上,造成了测试信息的孤立,无法对所有测试信息进行查看、统计等;部分测试设备的测试数据信息会自动覆盖掉上次的测试结果,造成信息的丢失。为解决以上数据异构、信息孤立和信息丢失等问题,使装备所有测试信息得到共享,为机关、技术人员的管理和质量检测服务,需要对测试信息进行挖掘,研究导弹保障装备测试信息进行集成开发平台,为信息共享提供技术支持。

## 2 系统开发

### 2.1 系统开发的结构

由于导弹测试设备是分布式的,部队现有的软件使用、管理人才不兼备,随着部队建设的发展,有可能引入新型的导弹及相应的测试设备等,需要开发一种入网简单、易于维护的系统进行管理,比较现有的网络实现的两种模式: B/S 结构模式和 C/S 结构模式的优缺点,选择 B/S 结构,即 Browser/Server (浏览器/服务器) 结构,它对于导弹测试信息管理来说有很多的优点。

1) 安装简单,只要客户端安装了浏览器(比如 IE),就可以对系统进行访问,而不需要部队再在客户端安装专门的程序。

2) 维护容易,由于软件都是在服务器上布置的,出现问题时仅需要将服务器上的应用程序进行检测即可。

3) 拓展方便,部队如果需要将一台主机连接入网,只需给要入网主机分配一个未占用的 IP 地址,通过网线连接到端口即可。

### 2.2 系统开发的平台

#### 2.2.1 网络平台—虚拟Internet

虚拟 Internet 是指把 Internet 技术应用于局域网内部的一种信息管理和交换平台,是在传统局域网的基础上,采用 Internet 技术和标准来构筑或改建成可以提供 WWW 信息的一种应用。虚拟 Internet 的网络基础是一个局域网,可以是对等网,也可以是客户机/服务器网络,在导弹保障装备测试数据管理系统中采用了 B/S 结构基础上的 WWW 服务进行数据的管理,这种结构把数据处理大部分集中到服务器,在客户端仅进行一些简单处理。

#### 2.2.2 数据库平台—Oracle 9i

Oracle 数据库是一种关系型数据库,它在数据安全性和数据完整性控制方面具有独特的优越性,另外它还具有跨越操作系统、多硬件平台的数据相互操作的特点,所以越来越多的用户将其作为数据的后台处理系统。Oracle 数据库的主要特点有: 支持多用户、大事务量的事务处理;数据安全性和完整性控制;提供对数据库操作的接口;支持分布式数据处理;可移植性。

#### 2.2.3 操作系统平台

在局域网中服务器端操作系统为 Windows2003

Server, 该操作系统遵循 TCP/IP 通信协议, 提供了多种网络技术与服务, 可以配置多种不同结构的网络, 如 Intranet、Internet、Extranet 和远程访问, 可以配置成为多种服务器, 如 IIS、FTP、SMTP、NNTP 等; 客户端操作系统为 Windows XP, 利用其自身组件 Internet Explore 可以浏览、访问服务器上的网页。

#### 2.2.4 Web服务器软件—IIS

IIS 是微软的一个 Web 发布服务器, 是 Internet Information Server 的缩写, 它是一个标准的网站服务器, IIS 是和 Windows 服务器操作系统紧密的结合在一起的, 然后在服务器上建立相应的网站。IIS 的组件以服务程序的形式在后台执行, 就像驱动程序一样是操作系统的一部分, 具有在系统启动时被同时启动的服务功能。客户端利用 TCP/IP 协议连接上 IIS, IIS 通过超文本传输协议 (HTTP) 传输信息, 还可配置 IIS 以提供文件传输协议 (FTP) 和其他服务, 如 NNTP 服务、SMTP 服务等。

#### 2.2.5 ASP.net程序运行环境—.NET Framework

.NET Framework 是 COM 架构的扩展, 是 MicroSoft.NET 结构的核心, 它区隔了操作系统和所有以 .NET 开发出来的应用程序, 是一个安全、高性能与扩展性佳的运行环境, 支持统一的类库, 如供 VB, C#, VC 等语言调用。最低层是一个通用语言运行环境, 在执行时管理代码的代理, 提供内存管理、线程管理和远程处理等核心服务, 并且还强制实施严格的类型安全以及可提高安全性和可靠性的其他形式的代码准确性; 中间层是 .NET Framework 类库, 提供许多类和接口, 例如 ADO.NET、XML、IO、网络、安全、多线程等。最上层是用户接口与应用程序接口, 其中的“Web Forms”、“Web Service”组成了全新的因特网应用程序接口, .NET Framework 将其统称为“ASP.net”。

#### 2.2.6 ASP.net程序数据库访问方式—Oracle Client.NET

OracleClient.NET 的对象模型主要包括以下几个部分。

OracleConnection 用来创建连接到 Oracle 数据源的数据链路; OracleCommand 用来对数据源执行 SQL 命令并返回结果; OracleDataReader 用来提供

顺序的只读的数据; OracleDataAdapter 用来对数据源执行 SQL 命令并返回结果, 但必须与 DataSet 对象配合使用。DataSet 对象是 ADO.NET 的核心包含了数据表 DataTable 和 DataRelationship 两个对象。

#### 2.2.7 ASP.net程序开发平台—Visual Studio.Net

Visual Studio.NET 是 .NET 平台下最为强大的开发工具, 是一套多语言系列的编程工具。Visual Studio.NET 提供了包括设计、编码、编译调试、数据库联接操作等基本功能和基于开放架构的服务器组件开发平台、企业开发工具和应用程序重新发布工具以及性能评测报告等高级功能。Visual Studio.NET 内含的各种语言又可以进行各种项目 (控制台应用程序, Windows 应用程序, Web 应用程序等) 的开发。

#### 2.2.8 ASP.net程序开发语言—C#

C# 是一种现代的、面向对象的程序开发语言, 它使得程序员能够在新的微软 .NET 平台上快速开发种类丰富的应用程序。利用 .NET 平台提供的大量工具和服务, 能够最大限度地发掘和使用计算及通信能力。C# 是 .NET 的关键性语言, 它是整个 .NET 平台的基础, C# 具有以下突出特点: 语法简洁, 面向对象, 与 Web 紧密结合, 完整的安全性及错误处理, 版本控制, 灵活性与兼容性。

### 2.3 关键技术

#### 2.3.1 异构数据的转化和统一存储

异构数据的转化和统一存储是系统实现的关键, 按照系统开发的顺序分为三步: 确定统一的数据格式, 测试数据从文件中的提取和提取数据的存储。

##### ● 确定统一的数据格式

测试设备的多样化带来了测试数据文件的多样化, 但是数据文件里面都包含了需要测试的信息的字段, 在 oracle 数据库表设计时通过对这些测试字段进行汇总和分析提取, 确定数据库表的字段, 从而在不丢失测试数据信息的前提下实现了统一的数据存储格式。

##### ● 测试数据从文件中的提取

测试数据文件有常见的 Excel 文件、FoxPro 数据库文件、Access 数据库文件和记事本文件, 还有

测试设备软件编写人员自己定义的二进制 dat 文件,对于常见的文件格式,调用 Oledb 或 Odbc 数据连接程序可以将数据文件的各个字段读取出来存储到内存里面,而对于二进制的 dat 文件,一般分以下几步进行数据的提取:确定记录长度,确定记录数,参照打印结果分析某一记录来确定记录中的字段,明确各个字段在记录中的位置,明确各个字段的存储码,通过这样一个由大到小,由粗到细的过程即可将测试数据信息从文件里面提取出来存储到内存。由于常见的数据文件的字段名称和字段在表里的顺序也不尽相同,二进制文件更是如此,所以针对某一测试设备就有一个数据转化接口来实现文件中测试数据的提取。

#### ● 提取数据的存储

提取出来的数据是暂时存储在服务器内存上的,根据数据文件特点的不同,数据有的以数组形式存储,有的以 DataSet 形式存储,利用 Oracle Client.NET 数据提供程序包含的数据库操作的类实现数据由内存向数据库的存储。

### 2.3.2 存储数据的查看和挖掘

数据的异构转化和统一存储实现了测试数据的收集,对这些数据的利用,数据查看是其最简单的

功能,还可以对这些数据进行深层次的挖掘。

数据查看是对存储在数据库中的数据进行查询,将查询结果显示给系统用户,这一简单用途主要供数据上传者查看自己上传的信息。

数据挖掘是对收集信息进行统计、变换得到需要的信息,比如可以统计出所有测试项目中测试不合格率最高的项目提供导弹重点维护信息,通过对某一导弹的各个项目测试数据的变化态势预测导弹的健康状况,通过对所有测试项目的合格率提供合格导弹数目信息等等。

## 3 结论

本系统的实现能够将测试数据信息有效保存下来进行统一的管理,是信息化实施的初级阶段,在收集的数据基础上对有用信息进行深层次的挖掘,提供利于作战决策的重要信息是信息化的最终目标。

## 参考文献

- [1] 戴有炜编著.Windows Server 2003 网络专业指南[M]. 北京:清华大学出版社,2006
- [2] 飞思科技产品研发中心编著.Oracle9i 基础与提高[M]. 北京:电子工业出版社,2003
- [3] 杨鲲鹏,孟凡琦,温才毅编著.ASP.NET+SQL Server 动态网站开发从基础到实践[M]. 北京:电子工业出版社,2005
- [4] 林邦杰编著.深入浅出 C#程序设计[M]. 北京:中国铁道出版社,2005

## 作者联系方式

通信地址:山东烟台海军航空工程学院

邮政编码:264001

联系电话:0535-6635910

# 美国防部联合互操作性测试的实施及特点

张海翔 邹江南

**摘 要：**美军参联会和国防部规定，国防信息系统局联合互操作性测试司令部是所有信息技术和国家安全系统互操作测试的权威部门。主要系统设备在装备使用前必须要通过联合互操作性司令部的测试认证。

**关键词：**美国防部；联合互操作性；测试；认证

## 1 美军互操作性测试认证的强制性

美军将所有 C<sup>4</sup>ISR 网络系统、计算处理系统和相关的电子信息设备统称为信息技术和国家安全系统（IT/NSS），而联合互操作性测试则是保证信息技术和国家安全系统能否正常运行，能否互联

互通的不可或缺的手段（图 1）。为保证全球信息栅格和网络中心战的实现，进而为美军全球作战提供强有力的支持，美军参联会和国防部发布了一系列文件，对美军互操作性测试认证必要性进行了严格的强制规定。

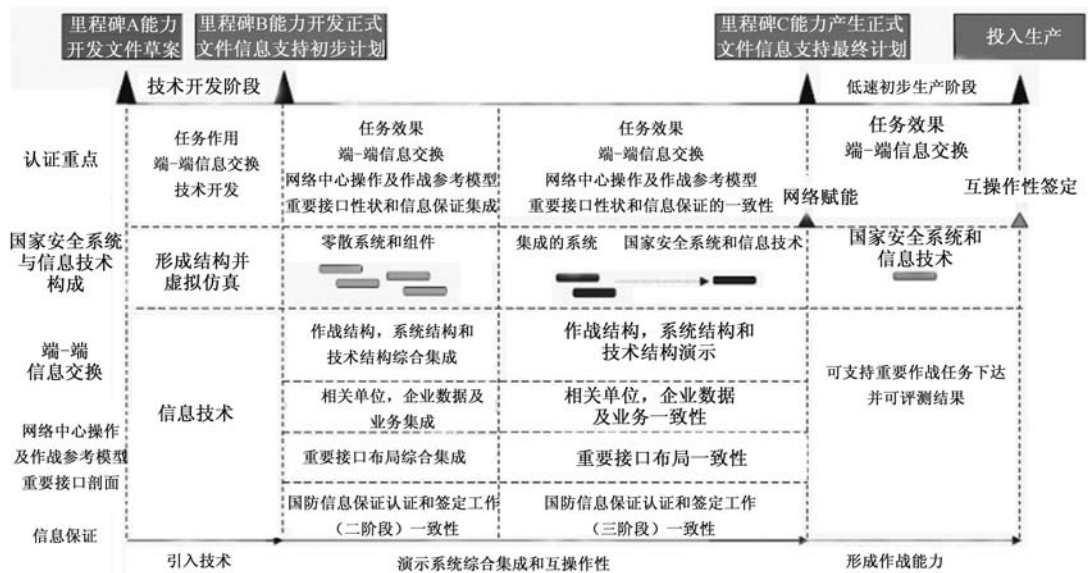


图 1 美军电子信息装备发展测评重点流程图

2004 年 6 月美国防部第 4630.8 号指示：所有信息技术和国家安全系统在装备部队前必须通过国防信息系统局联合互操作性司令部试验和测试。

2006 年 3 月 美参联会主席第 6212.01D 指令：所有信息技术和国家安全系统必须经由国防信息系统局联合互操作性测试司令部评估认证。

同一时期，美参联会主席手册（CJCSM）和国防部指令（DOCC）就美军互操作性测试进一步明确指出如下几点。

1) 联合互操作性测试不是替代通信电子部门

的系统确认。在联合能力综合和开发系统（JCIDS）程序中必须同时得到联合互操作司令部的联合互操作性测试和装备部队前通信电子部门的认可。所有系统，包括采办类型、非采办类型和将要推广的系统（含最初产品和更新产品），在装备使用前必须评估认证。

2) 同一个系统设备（网络设备）在不同时期、不同环境条件下，其互操作性是变化发展的。在系统整个寿命周期定期进行联合互操作性测试认证，可及时掌握系统在变化了的信息环境条件的最

新状况，所以在其整个寿命周期中至少每三年进行一次互操作性测试。

3) 信息技术和国家安全系统的具体标准、与全球信息栅格的一致性及互操作性测试评估计划的拟定及实施，都要由国防信息系统局联合互操作性测试司令部负责。例如，根据美地理空间与图像标准管理委员会（G/ISMC）现行政策，特别是为了维持统一性和可操作性，美国各情报机构，包括国防部和美政府部门相关部局，都要采用由国防信息系统局联合互操作性测试司令部拟定的美国国家图像传输格式标准。

2 联合互操作性测试司令部

联合互操作测试司令部（JITC）是美国国防部测试与评估执行机构下设的两个主要单位之一，是独立的信息系统认证评估部门，也是一个对将要进入全球信息栅格（GIG）网络系统设备进行信息保证（IA）和互操作性（IOP）验证的权威性负责单位。联合互操作性测试司令部主要任务包括：担任国防信息系统局以及国防部其他 C<sup>4</sup>I 采购事项独立的操作测试与评估；确定并解决 C<sup>4</sup>I 与战斗支援系统互操作性的不足；提供 C<sup>4</sup>I 联合与综合互操作性测试、评估与认证；为作战司令部、各兵种以及各部局提供互操作性支持、战场评估和技术协助；为美军 C<sup>4</sup>I 系统提供相应的训练保证。

联合互操作性测试司令部设有计划、政策与作战人员支援部、自动化系统与测试支援部、华盛顿执行部、战斗支援与情报部、网络与传输部以及操作测试评估部等单位。该司令部在美本土设有三个主要测试基地，（亚利桑那州瓦丘卡堡、马里兰州

印第安黑德和弗吉尼亚州福尔斯彻奇）编配各类技术人员约 1300 人。

事实表明，联合互操作性测试司令部通过为美军所有重要电子信息系统的寿命周期进行程序与产品评估、操作分析和技术辅助，为美军作战人员降低风险提供了极为有力的支持。

3 互操作性测试一般要求及实施

美军国防部文件为互操作性的定义是：系统、分队或部队向其他系统提供（或接收其他系统的）数据、信息、装备和业务，并能与之（其他系统）有效交互使用的能力。信息技术和国家安全系统互操作性包括信息在技术上的交换和完成任务所要求的信息交换端-端操作的有效性。需要重视的是，美军近期产生的指导性文件多次指出，互操作性远不只是信息交换。它还包括系统的整个寿命周期以及与信息保证相适应的系统、处理、程序、编制和任务。

美军认为，通常意义上的联合互操作性测试认证只是通信与信息系统全部认证过程的一部分，而在网络中心战背景下，测试评估部门更强调其在作战环境下的互操作性能力，评估的重点是不同环境下对作战的影响。在目前的条件下，有关互操作性测试的认证还有通信电子部门（J6）的互操作性和保障性认证，通信电子部门的系统确认。通信电子部门认可的互操作性需求和能力将用于联合互操作性测试司令部互操作性测试和评估。反过来，联合互操作性测试司令部得出的测试结果也将用于通信电子部门的确认程序和里程碑决策部门（MDA）的装备推广应用决策。

表 1 网络准备主要性能完备时的测试环境演变

网络准备主要性能 参数要点	测试环境	负责单位	测试环境和状态
端-端信息交换	联合任务环境	相关功能性委员会和联合能力 领域单位	根据需求发展
网络中心战和网络 中心作战参考模型	相关单位参考执行	联合能力领域和 相关单位	相关单位管理方法成熟
	网络中心战企业服务通过全球 信息栅格联合开发与认证环境 参考实施	国防信息系统局	全球信息栅格联合开发与认证环境 下的军事行动方案需要网络中心战 企业服务
重要接口布局	全球信息栅格联合开发与认证 环境以及国防部实验室	国防信息系统局与重要接口布 局发起者	重要接口布局参考实施发展缓慢
信息保证	作战网络	作战测试机构和委托授权单位	适当的位置



美军还认为，在信息网络高度发达的今天，美军作战部队对增强联合、可互操作的 C<sup>4</sup>ISR 能力从来没有如此迫切，条令、编制和训练对信息系统装备的效能发挥同样也产生了极大影响。所以，国防信息系统局更加强调联合互操作测试司令部对美军四个军种、作战司令部和国防部及联邦各部局的全方位直接支持，联合互操作性测试的内容已不仅仅局限在美国国防部有关单位和部门通过采购得到或在用的所有信息技术和国家安全系统（系统或业务）

产品，不仅仅包括联合网络基础设施系统组件、加密设备、网络路由器和网络防火墙，还包括了各种渐进式开发在内的采购策略加强状况，以及不同背景条件下的系统情况对网络准备（Net-Ready）的影响，比如：条令、编制、训练、装备、领导、人员和设备（DOTMLPF），也包括硬软件改造或其他条件下的系统状况。上表（表 1）为美军根据不同测试环境、不同背景拟定的测试框架性要求。

表 2 网络准备主要性能特性

主要性能特性（KPP）	界限 （Threshold）	目标 （Objective）
网络准备： 系统必须能保障以网络为中心的军事行动。系统必须能接入网络并在网络中受到管理，以保密方式交换数据，增强任务有效性。 系统必须能为网络中心军事行动提供不间断、可靠、可互操作、保密且高效运行的信息交换。	在联合和系统综合结构中，系统必须完全支持执行联合的重要作战行动识别，必须满足向网络中心军事行动技术需求的过渡。包括： 1）技术体系结构（TV-1）确定的国防部信息技术标准注册（DISR）命令中全球信息栅格技术标准及布局； 2）重要接口布局通告中确定的国防部信息技术标准注册命令全球信息栅格重要接口布局认定； 3）网络中心战及作战参考模型企业服务； 4）信息保证需求，包括：可用性、完整性、鉴别、保密和不可抵赖，并通过指定的批准授权单位公布应用过渡认可（IATO）； 5）作战效能信息交换、任务重要性能和信息保证分发、数据校正、数据可用性，以及特别是在联合和系统集成结构应用中的始终如一的数据处理。	在联合和系统综合结构中，系统必须完全支持执行全部作战行动识别，必须满足向网络中心军事行动技术需求的过渡。包括： 1）技术体系结构（TV-1）确定的国防部信息技术标准注册（DISR）命令中全球信息栅格技术标准及布局； 2）重要接口布局通告中确定的国防部信息技术标准注册命令全球信息栅格重要接口布局认定； 3）网络中心战及作战参考模型企业服务； 4）信息保证需求，包括：可用性、完整性、鉴别、保密和不可抵赖，并通过指定的批准授权单位公布应用过渡认可（IATO）； 5）作战效能信息交换、任务重要性能和信息保证分发、数据校正、数据可用性，以及特别是在联合和系统集成结构应用中的始终如一的数据处理。

联合互操作测试司令部组织的联合互操作测试是根据美军联合参谋部通信电子部门认可的网络准备主要性能参数（NR-KPP），以及其他得到批准的需求。为节省资源，实际的测试工作也可以与其他测试活动（开发测试评估和作战测试评估）一并进行。联合互操作测试司令部作为联合互操作性测试的组织实施部门，在相关单位提供的测试结果充分可靠时，也可以将这些成果作为联合测试的基础。美军强调，联合互操作测试及认证是一个持续的过程，必须对系统的整个生命周期进行管理并提取资源。同时，在系统需求认证的可用性方面则要求能用于联合/企业级信息交换的所有系统，并且在投入使用前必须进行网络准备认证。美军目前联合互操作性测试认证主要集中于网络准备主要性能参数的三个方面（参见表 2）。

1）与网络中心作战及网络中心战的（Net-Centric Operations and Warfare, NCOW）参考模型

的一致性；  
2）利用所赋予的能力，有效联接信息交换和操作，保障支持综合体系结构产品；  
3）与可用的全球信息栅格重要接口布局（KIP）一致；同时要验证与国防部信息保证需求的一致性。

4 部分互操作性测试成果

美军联合互操作性测试司令部测试计划安已排至 2010 年。前期完成的代表性测试认证包括如下几个方面。

（1）联合战区防空与反导战术数据链  
2003 年以来，国防信息系统局联合互操作测试司令部测试设备与美军其他军兵种和国防部有关部局的测试设备实现链接。这种极有成效的分布式

网络对联合战区防空与反导（JTAMD）战术数据链系统进行了连续测试，效费比令美军高层极为满意。为此，美国防部要求联合互操作测试司令部进一步链接综合性的联邦战斗实验室网络，以便对不是美军的系统和设备进行分布式的互操作测试评估。

(2) 在线认证协议与美国防部公钥基础设施

2004 年 2 月 19 日至 4 月 40 日，联合互操作测试司令部公共密钥赋能（PKE）应用实验室对 Ascertia TrustFinder 在线认证协议（OCSP）Server 4.0 进行了测试。测试的目的是验证 Ascertia TrustFinder 在线认证协议 Server 4.0 能否与美国防部公钥基础设施（DOD PKI）实现互操作。联合互操作测试司令部在测试最终报告中指出，Ascertia TrustFinder 在线认证协议 Server 4.0 可以支持所有强制性需求和部分非强制性需求，通过了互操作性测试。

(3) IPv6M/T 路由器

2007 年 5 月，Juniper 网络公司研制的 IPv6 M/T 系列路由器平台通过了联合互操作测试司令部的认证。成为 IPV6 获准产品名单（APL）中的第一个产品，为美军应用 IPv6 系统迈出了重要的一步。据此，美国国家信息基础设施国防部长办公室（OSD-DII）训令再次强调，所有国防部计划管理人员的产品采购，都要遵从国防部国防干线传输网络在 2008 年实现从 IPV6 转换成 IPV6 战略发展计划。

5 国防部联合互操作性通信演习

为对美军已装备部队或新近进行了升级改造、或对厂家新研制系统进行最后的野战环境测试，美军每年（2 月~4 月）都进行一次综合性的大规模国防部联合互操作性通信演习（DICE）。由于演习极为贴近实战，美军在演习过程中对互操作性测试的三个重要组成部分：参演部队、操作规程和设备配置特别关注。参加演习的部队包括美军各军兵种，演习所用设备系统通常也都由作战部队安装、操作和维护，台站的装备配备也都按实战或应急响应使用要求配置。由于演习环境和场景的真实，一

参考文献（略）

作者联系方式

通信地址：北京市丰台区大成路 13 号 X01      邮政编码：100039      联系电话：010-66820342

方面，所得到的数据对系统的互操作性有贴切的反映，可有效克服系统和设备设计上的不足；另一方面，操作人员对所配备系统的战术、技术和程序是最直接的学习掌握，也为参加演习的部队提供了宝贵的训练机会。有材料表明，尽管美军各军兵种由于作战使命和作战任务不同，对联合互操作演习的期望点也有所不同，但联合互操作演习对美军各军兵种使用现役装备实现互联互通，确实起到了近似实战条件下的检验和验证。

美军 2007 年联合互操作性通信演习的重点主要有三项：①进行多军兵种联合系统互操作性测试；②验证国防部同本地、国家、联邦、盟军设备与系统的重要接口；③支持战术部队训练而提供设备和场地。参加演习的测试项目达 53 个。其中有 10 项来自认证推荐部门，1 项是根据通用交换中心的建议、10 项互操作性改进评估、7 项演示、12 项保障业务和 14 项训练项目（参见表 3、4）。

表 3 2007 年 DICE 美军参演部队和主要参演装备

美军参演部队	主要参演装备
联合通信保障分队	四波段双集线器终端（QUHT）/iDirect 时分多址系列网络电话
陆军	AN/TSC-156 SHF 三波段卫星通信终端、数据组件、AN/TTC-56 单方舱交换设备和 AN/TSC-85 卫星通信终端
海军	水面指挥控制平台、AN/WSC-6 SHF 卫星通信终端和 Definity 综合业务数据网交换设备
海军陆战队	MSQ-126、数字技术控制设备、战术数据网信息保证设备、联合加强型核心通信系统 Block II 型
空军	战场可运式综合通信接入成套设备（TDCICAP）、保密话调制解调器、AN/TSC-152 / AN/USC-59 轻型多波段卫星终端和网络测试模块

表 4 2007 年 DICE 参演单位和系统数量

参演单位	参演系统数量
国防部及联合单位	8
陆军	12
海军和海军陆战队	1/3
空军	2
海上警卫队	3
国家安全部门	8
民用授权单位	6
卖方	10

# 数据质量管理的研究与实现

张红亮 罗强一 曹京春

**摘 要:** 数据质量管理是数据建设中的重要工作, 数据质量管理体系集中体现了对数据质量的管理要求, 既为数据维护人员检测、记录、跟踪数据问题提供手段, 也是数据主管部门评价数据质量的重要依据。本文初步定义了数据质量指标体系, 并探讨了数据质量管理体系的实现与应用流程。

**关键词:** 数据工程; 数据质量管理; 指标体系

## 1 引言

数据质量是一个广义的概念, 是数据产品满足指标、状况和要求能力的特征总和。不仅要考虑与质量相关的各个方面, 而且强调数据满足使用者的需求。系统研制的最终目的是对使用者关心的数据完成各类静态或者动态的处理或管理任务, 为使用者创造预期的和附加的价值, 因此有关数据质量的指标参数是使用者最为关心的指标参数。通过数据质量信息和相关的指标参数, 使用者可以了解到数据的正确性、完整性、一致性、精确性、有效性, 数据生产目的、用途以及数据日志等相关信息。

虽然, 学术界已经对数据质量问题进行了大量的研究工作, 也取得了很多成果, 但在指导实际应用上, 还存在较大的差距。现有的数据库系统一般对数据质量做出了某种程度的表达, 但尚缺乏在具体的数据活动中将数据质量要求作为主线, 构建必要的数据库质量指标评价体系。数据库系统如果作为决策支持系统的基础, 就必须提供高质量的数据和服务。因此, 数据质量是提高军事信息系统应用水平和亟待解决的关键问题, 也是所有各类信息系统面临的一个共同难题。

在军事应用领域, 随着军队信息化建设的逐步深入, 数据在各类军事行动和日常业务工作中的作用越来越重要, 数据对指挥决策的正确性和军事行动的效果影响也越来越大。因此, 数据质量管理对发挥军事信息系统得整体效益起着关键的作用。

## 2 数据质量指标体系的定义

确定数据质量指标体系是一项重要, 但又常常

被忽略的工作, 为任何一个信息系统定义数据质量指标体系从来都不是一个简单的任务。数据质量的概念是相对而言的。正如不同的使用者对数据本身的理解是不同的, 对数据质量指标的要求当然也就随着观察对象或使用者的不同而不同。

为了便于综合评价, 可以将数据质量指标分为数据构造质量指标和数据使用质量指标两个方面。

1) 数据构造质量指标: 存在于数据库其他模块对数据的操作当中, 是反映数据库物理层数据的固有属性。可分为数据的完整性、精确性、一致性以及唯一性等。其中具体的指标特征和度量可以按照如下定义。

a) 正确性: 数据按要求录入和应用, 没有出现录入错误、关系表达正确、计算公式准确。其度量指标可以是出现问题的数目。

b) 完整性: 实体的属性是否可以被完整地与数据需求相对应, 如标准值数据域中是否包含了所有的标准值。其度量指标可以是现有数据域与实际需求数据域比较时, 正确值的百分比。

c) 一致性: 数据应该符合一致性约束条件。其度量指标可以依据一致性约束条件来拟定, 检查包括数据的形式和内容两个方面。其度量指标可以是出现问题的数目。

d) 精确性: 数据的精度能够满足对数据的需求, 如经纬度的小数保留位数, 实时记录是否到秒等。其度量指标可以是现有数据精度当与实际需求精度比较时, 正确值的百分比。

e) 唯一性。同一类中的数据仅有一个指定的值, 没有不相同或不等值。其度量指标可以是有唯一的主关键词的记录百分比。

2) 数据使用质量指标: 主要分为数据的有效

性、适用性、可理解性、时效性、集成性和安全性等。其中具体的指标特征和度量可以如下定义为。

a) 有效性：一是数据是合理的、准确的，可以被理解和应用的，并且是经过审核和批准的。其度量指标可以有值的数据百分比，并且该值属于可允许值的域。二是数据是有用的，可用采集到的数据是否在数据库中得到应用来衡量；其度量指标可以是数据查询率。三是数据是够用的，数据的应用可以满足使用中的各种要求。其度量指标可以是不能满足使用要求的问题数量。

b) 适用性：数据能满足业务需求，并且遵循所要求业务规则，适用于指定业务。其度量指标可以是现有数据关系、触发器、存储过程的设置与业务规则比较时，正确值的百分比。

c) 可理解性：一是数据可以在数据字典/模式中编成文档。其度量指标可以是现有文档和实际要求比较时，正确值的百分比。二是使用者对于数据的展现方式和从该数据中导出的信息感到满意的程度。

d) 时效性。数据的敏捷性、可响应性、数据更新契机、信息有效期，数据应该是及时更新和保鲜的。实效性是主观概念，由数据的使用者来决定。其度量指标可以依据对数据的更新需求的时间要求或时间范围，如月、日、时、分、秒等来拟定。

e) 集成性：较少的冗余数据、数据不一致的可能性比较小、接口程序少、时间不一致的问题比较少、更多的及时数据。其度量指标可以是系统的开放程度，设计与实现上的规范程度，接口与交换中的标准化程度。

f) 安全性：数据有可靠的存储备份措施，数据是受控的，数据的使用是可以追溯和审计的，数据在安全和保密上达到有关要求。

### 3 数据质量管理系统的设计与实现

数据质量管理系统是用于检测、记录、跟踪、统计数据质量问题的数据库军事信息系统。它通过分析影响数据质量的各种因素，建立数据质量指标体系，对数据处理多个环节中的数据质量进行检测和控制，辅助数据维护人员对数据的重复、缺失和异常进行记录和管理，为保证和评价作战数据的质量提供支持。

### 3.1 主要功能

数据质量管理系统应该包括以下主要功能，如图 1 所示。

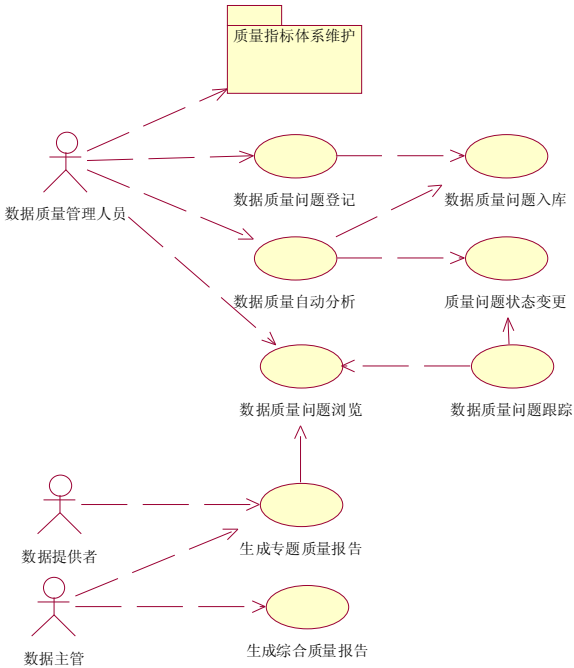


图 1 系统主要功能及相互关系

#### (1) 数据质量指标体系维护

本功能包括通用指标维护、元数据维护、质量规则维护、专用指标维护等四个子功能，具体如图 2 所示。

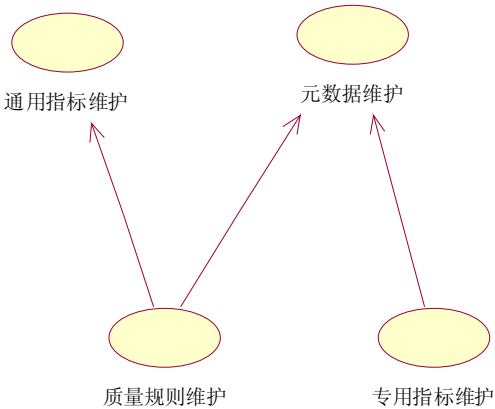


图 2 数据质量指标体系维护功能

通用数据质量指标是指从某些相似的具体规则中抽象出来的共性指标，这些具体的规则通常描述相似的属性，以及相同的评判算法。通用数据质量指标和元数据相结合就可形成具体规则。

专用数据质量指标是指与具体属性联系及其紧

密的指标,体现了具体属性的特性和要求,无法应用于其他属性,也无法进行抽象。专用数据质量指标本身就反映了具体规则。

数据质量指标体系维护的主要工作包括:

- 通用指标维护:建立并维护通用数据质量指标,并对每一指标定义积分权重、错误等级、依赖的参数和评判算法。
- 元数据维护:获取标准目标数据结构,包括表和字段的定义,以及它们之间的从属关系。
- 质量规则维护:建立通用指标与元数据的关联,在具体字段上应用一项或多项通用指标,包括这些指标需要明确的参数,形成可操作的数据质量规则。
- 专用指标维护:在元数据基础上,建立并维护通用数据质量指标,并对每一指标定义积分权重、错误等级,自动建立与元数据的关联。

#### (2) 数据质量问题登记

提供用户界面,允许用户以人工的方式登记发现的数据质量问题(调用数据质量问题入库)。选择问题类型时,可以选择与结构绑定的质量规则(含专用指标),也可选择与结构无关的通用指标(不含专用指标)。用户还可以登记参考值。

#### (3) 数据质量自动分析

按照数据质量规则(仅限于可自动检验的规则),并依据规则对应指标的评判算法,对目标数据进行自动检查和分析,发现新的问题自动登记入库(调用数据质量问题入库);复查已有问题的改正情况,并自动更新其状态(调用数据质量问题状态变更)。

#### (4) 数据质量问题入库

提供功能接口,把数据质量问题存入数据库中。对问题类型的描述应该以质量指标为准,而非质量规则。

#### (5) 数据质量问题浏览

选定某一数据提供单位,对该单位的数据质量问题进行浏览;通过数据质量问题列表,可以进行数据质量问题跟踪。

#### (6) 数据质量问题跟踪

提供用户界面,查看问题详情和问题数据内容,确认无误后完成变更(调用数据质量问题状态变更)。

#### (7) 数据质量问题状态变更

提供功能接口,对数据质量问题的状态进行变更。

#### (8) 生成专题数据质量报告

对于不同数据提供单位,分别生成专题数据质量报告。也可对单个数据问题,单独生成数据质量报告。把专题数据质量报告反馈给数据提供者,使其可根据报告,对问题进行改正;首长可通过专题报告,了解数据提供单位上报数据质量的具体情况。

#### (9) 生成综合数据质量报告

根据发现的问题及改正情况,加权计算得出评分。通过对提供单位进行比较,为数据主管提供综合质量评价,作为奖惩的依据。

### 3.2 应用流程

系统的主要角色有数据提供者、技术审核人员、业务审核人员、数据主管组成,应用流程如图3所示。图中灰色活动不属于系统功能范畴。

数据提供者上报数据。

业务审核人员进行数据质量自动分析,登记新发现的问题,并追踪未改正的问题。

技术审核人员使用数据维管工具进行技术性检查,登记新发现的问题,并追踪未改正的问题;业务审核人员使用其他军事信息系统进行数据真实性审核,登记新发现的问题,并追踪未改正的问题。

技术审核人员对不同的数据提供者,分别生成不同的专题质量报告,把数据质量问题反馈给数据提供者;

数据提供者改正问题后,再次上报。

全部问题改正后,技术审核人员生成综合质量报告和专题质量报告,并呈报数据主管进行讲评。

### 3.3 数据结构

系统数据库的实体包括:质量指标、目标元数据、质量规则、质量问题。

质量指标描述了抽象的通用指标和具体的专用指标,应该包含指标名称、严重等级、评分权重、评判算法等属性。

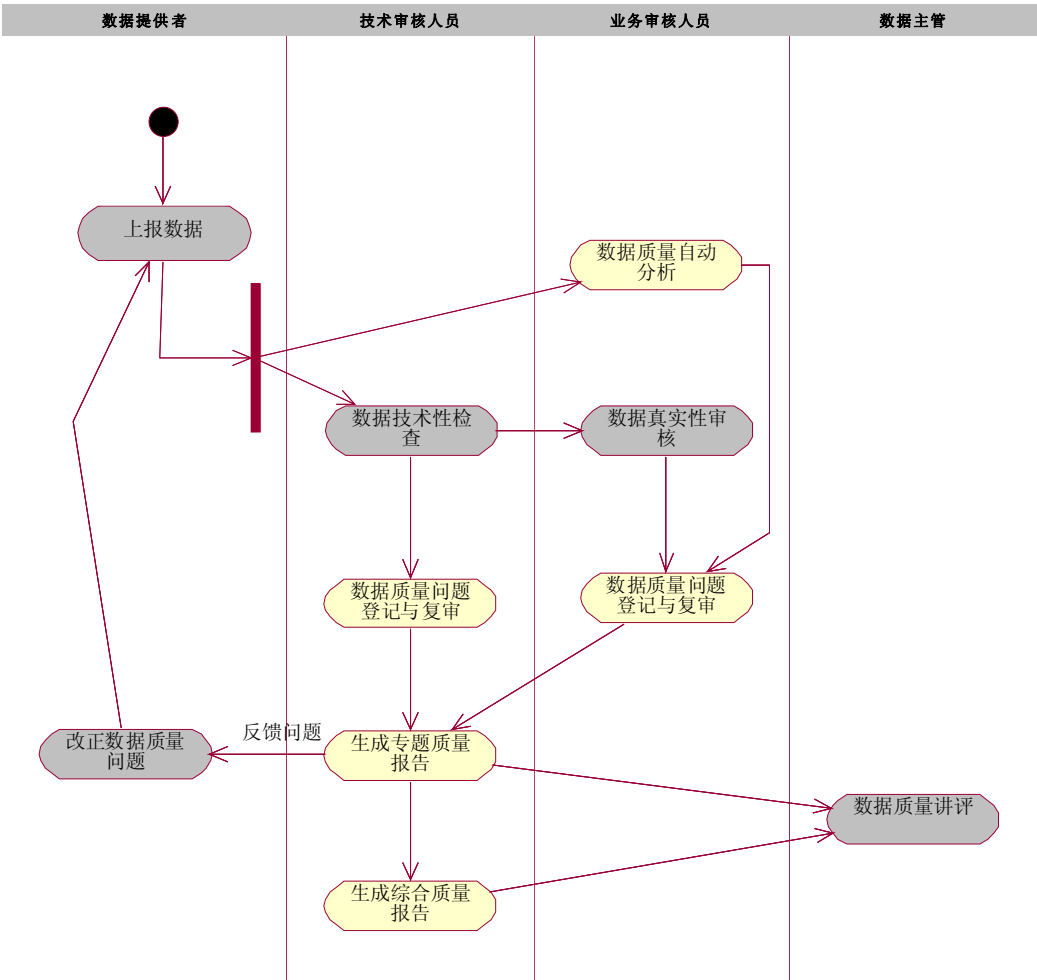


图3 应用流程图

目标元数据描述了目标模型的元数据，应该包含目标模型的表和字段定义。

质量规则是指质量指标与元数据的关联，适用于自动分析和登记问题，而不适用于问题的评价。质量规则应该描述指标、字段和指标参数等属性。

质量问题记录了所有的数据质量问题，应该包含提供单位、数据批次、违反指标、指标参数、问题表、问题字段、问题记录主键、参考值等属性。

4 小结

数据是军事信息系统的基础，没有准确的数据，军事信息系统的作用就大打折扣。必须高度重视数据质量工作，而数据质量管理体系为发现数据中的各种问题提供了重要的手段，为保证数据的质量起到重大的作用。数据质量管理体系的研究与实现，对于改善数据质量，提高军事信息系统的整体效益具有非常重要的意义。

参考文献（略）

作者联系方式

通信地址：北京市丰台区大成路13号R03  
邮政编码：100039  
联系电话：010-66820273-802

# 炮兵指挥信息系统综合集成研究

赵鑫 闫耀祖 陈涛

**摘要：**对炮兵指挥信息系统的综合集成，是体系重构、结构优化、功能扩充的过程，应着眼炮兵作战理论的变革、炮兵武器平台可能的发展，同时借鉴外军指挥控制装备建设的有益经验，重点从体系结构、功能配置和软件功能三个方面进行综合集成。

**关键词：**炮兵；指挥信息系统；综合集成

炮兵是以火力遂行任务的战斗兵种，是陆军火力突击的骨干力量，是一化联合火力打击力量的重要组成部分。炮兵指挥信息系统是炮兵参与一体化联合作战指挥与实施炮兵作战指挥的技术支撑平台，是制约炮兵指挥效能的重要因素，其性能及体系结构对炮兵整体作战能力的发挥具有重大的影响。

## 1 炮兵指挥信息系统建设面临的形势

### 1.1 作战理论不断创新

随着信息要素在炮兵战斗力各要素中地位的不断攀升，建立在合同作战、机械化战争形态背景下的陆军作战理论，正向适应一体化联合作战的信息化陆军作战理论发展。就炮兵作战理论而言，信息化条件下的炮兵作战原则、作战方法等都注入了信息要素，与机械化条件下相比，更加强调信息主导、火力主战，高效的火力毁伤将是炮兵完成任务的主要方式。曾经在传统装甲机械化突击中发挥了重要的炮兵火力支援，将更多地让位于炮兵精确高效的火力毁伤。必须以创新的作战理论为指导，加速炮兵指挥信息系统的发展。

### 1.2 科学技术飞速发展

科学技术始终是指挥信息系统发展的推动力。不断将成熟的先进技术嵌入炮兵指挥信息系统，对于提升指挥信息系统的综合效能具有十分重要的作用。信息化战争需要的是融入了信息技术的信息化、智能化炮兵指挥信息系统。以信息技术为核心的现代科学技术，为炮兵指挥信息系统的综合集成提供了基础和保证，要把炮兵指挥信息系统发展的

基点定在提高其信息化水平上，以科技进步推动炮兵指挥信息系统不断向前发展。

### 1.3 武器平台性能不断改善

随着信息技术在炮兵武器装备上的广泛应用，炮兵武器平台的性能得到不断改善。在射击距离上，火炮的射程达到了近百公里，炮兵战役战术导弹的作用距离也增大到几百公里，炮兵既可以打击敌战术纵深又可打击敌战役纵深。在机动性能上，火炮机动速度的增大、克服地形障碍能力的增强，特别是以自主定位定向能力的提高，使其可以在机动中迅速投入作战。在射击精度上，激光末制导炮弹等一系列新型弹药的使用，也使炮兵的精确打击能力得到极大提升。武器平台性能的不断改善对炮兵指挥信息系统提出了更高的要求，炮兵指挥信息系统必须与炮兵武器平台的发展相适应。

### 1.4 综合集成方法日趋成熟

综合集成，是指科学与经验、定性与定量相结合，从而实现从局部定性认识上升到整体定量认识的系统方法。目前，综合集成的基本方法可以描述为：“对齐”、“瘦身”、“提升”、“填缝”、“绑定”。“对齐”是指统一技术体制，统一文电、态势、情报等作战数据格式。“瘦身”是指更换、合并低水平、低效益装备。“提升”是指通过硬件的更新、软件的升级对老装备进行改造，提升性能。“填缝”是指通过协议转换器、转换接口、网关等，实现两个或多个系统间的集成。“绑定”是指通过使用公共的平台，做到集成的系统互连互通。炮兵指挥信息系统涉及信息、火力、机动、防护等多个领域，包括作战、训练、维修、管理多个方面，只有



实行一体化的发展模式，走综合集成的路子，才能保证系统性，才不会顾此失彼。

## 1.5 综合集成是炮兵指挥信息系统发展的客观需求

我军炮兵指挥信息系统经过多年发展，已经拥有军（师）、群（团）和营（连）三级指挥信息系统，建立起了比较完整的作战指挥体系。但它们都是在当时特定的技术条件下研制的，随着科学技术的进步、作战理论的创新等多方面因素影响，使得现有炮兵指挥信息系统逐渐暴露出一些不容忽视的问题，如信息共享能力差、软件智能化程度低、辅助决策功能弱等，已经不能很好地满足部队的实际需求。因此，炮兵指挥信息系统必须进行综合集成，以更好地适应作战理论发展和部队作战行动的需要。

## 2 炮兵指挥信息系统综合集成的基本构想

未来我军炮兵指挥信息系统，是以计算机网络为核心，具备指挥控制、侦察情报、通信传输、安全保密、信息对抗等功能于一体的新型军事信息系统。对炮兵指挥信息系统的改造，应着眼炮兵作战理论的变革、炮兵武器平台可能的发展，同时借鉴外军指挥控制装备建设的有益经验，重点从体系结构、功能配置和软件功能三个方面进行综合集成。

### 2.1 炮兵指挥信息系统体系结构改造

对炮兵指挥信息系统体系结构的改造，要改变目前按指挥机构编成进行体系结构设计的状况，采取按炮兵作战指挥任务进行体系结构设计，构建战役炮兵作战指挥信息系统、炮兵战术指挥信息系统和炮兵武器平台控制系统的体系结构。以功能的强大和广泛的适应性满足不同战役（战斗）样式指挥的客观需要，以适应既有军师制又有军旅制等编制体制不同情况的需求。将现有的集团军炮兵作战指挥系统功能提升，既要适应集团军炮兵作战指挥的需要，又要适应集团军群、战区战略性战役炮兵作战指挥的需要；将现有的师炮兵作战系统和炮兵群（团）射击指挥系统合并，以满足战术兵团（部队）炮兵作战指挥的需要。炮兵营（连）射击指挥

系统将现有的营连子系统进行集成改造升级，并研制侦察指挥控制一体的武器平台控制系统，实现侦察与武器平台的无缝连接。

#### 2.1.1 战役炮兵指挥信息系统

战役炮兵指挥信息系统编配于集团军炮兵指挥部，供战役炮兵（集团军或集团军群）指挥机构作战指挥和训练使用，能够满足战役炮兵作战指挥的需要，保障战役炮兵指挥机构完成对所属炮兵部队的指挥与控制，组织战役炮兵火力与其他军兵种对地火力的协调。

#### 2.1.2 炮兵战术指挥信息系统

炮兵战术指挥信息系统既可编配于师炮兵指挥部，也可编配于炮兵群（团）指挥机构，供师炮兵、炮兵群（团）作战指挥和训练使用，能够保障战术兵团对编成内炮兵部队的指挥控制，提高战术兵团炮兵作战指挥效能。

#### 2.1.3 炮兵营（连）射击指挥系统

炮兵营（连）射击指挥系统编配于炮兵营连分队，供炮兵营（连）分队战斗指挥和训练使用，保障营（连）分队指挥员对所属炮兵分队及武器装备进行有效的指挥控制，提高炮兵分队遂行战斗任务的效能。

#### 2.1.4 炮兵武器平台控制系统

炮兵武器平台控制系统嵌入武器平台，在满足武器平台控制的基础上，还要具备一定的情报信息收集与传递功能，能够提供灵敏而准确的目标信息数据，近实时地送达指挥中心及炮兵武器平台，真正建立起“从传感器到射手”的信息渠道，实现对目标实施最有力而高效的打击。

### 2.2 炮兵指挥信息系统功能配置改造

对炮兵指挥信息系统功能配置的改造，要充分利用综合集成技术，基于战术互联网、数据链等信息传输设备，严格遵循指挥信息系统标准化建设的要求，在系统互连互通互操作的前提下，最大限度地提高系统技术综合集成化程度。准确把握各级指挥信息系统的功能需求，对操作席位进行重新设计和划分，提高席位的通用性。对系统功能配置进行整体优化，提升硬件设施的性能，精简设备和操作



人员,以适应指挥机构精干、小型、机动、多能的要求。

### 2.2.1 战役炮兵指挥信息系统

战役炮兵指挥信息系统由两辆车和相应的配套设备组成,即:一辆作战指挥车和一辆情报通信车,配套设备由检测维修和各种保障设备构成。系统共设置5个基本席位(指挥员席、综合计划席、指挥控制席、侦察情报席、通信保障席)和数个非固定席位(火力协调席、网管监控席、训练导调席等)。

### 2.2.2 炮兵战术指挥信息系统

炮兵战术指挥信息系统需一辆指挥情报车,配套设备由检测维修和各种保障设备构成。系统共设置3个基本席位:指挥员席、指挥控制席、侦察情报席,以及火力协调席和训练导调席等非固定席位。

### 2.2.3 炮兵营(连)射击指挥系统

炮兵营(连)射击指挥系统需配置一台高性能的便携式计算机,要能够为分队指挥员提供必要的图形、命令等显示和录入终端,为其指挥决策提供必要的支持。同时,应综合利用新型材料、主动防护技术等提高设备的防震抗毁及耐磨性能,减轻重量、缩小体积,既要便于携行使用,也要便于车载使用。

### 2.2.4 炮兵武器平台控制系统

炮兵武器平台控制系统与武器平台、信息采集传输设备合为一体,同时,要为武器平台操作人员提供命令、诸元等显示和录入终端,保障顺利操作武器平台,并能够在必要的时候进行人工干预。

## 2.3 炮兵指挥信息系统软件功能改造

对炮兵指挥信息系统软件功能的改造,要改变目前按指挥员、指挥机构工作内容程序进行模块设计的状况,采取按指挥员作战指挥决策流程即“目标信息处理—火力打击行动决策—毁伤效果评估”进行构件化改造、一体化整合,将系统软件主要划分为信息处理、指挥控制、效能评估、决策支持、专家咨询等几个模块,重点突出主要功能和决策支持模块的实用性,并从网络安全、通信保密等多方

面加强系统的安全防护。

### 2.3.1 战役炮兵指挥信息系统

对战役炮兵指挥信息系统软件功能的改造,应以战役炮兵作战指挥的根本职能为着眼点,以战役炮兵指挥员可向下指挥控制到基本的作战单元(炮兵营)为依据,在集团军炮兵作战指挥系统的基础上,同时减少对指挥员指挥决策辅助作用不强的功能模块,增加专家咨询模块和火力毁伤计算功能,改造升级部分功能模块,实现作战文书的代码化,使其能够满足战役炮兵指挥控制的需要。

### 2.3.2 炮兵战术指挥信息系统

对炮兵战术指挥信息系统软件功能的改造,重点要考虑到我军炮兵部队编制体制现状。在战术层面,我炮兵的编制较为复杂,平时编有集团军炮兵师(旅)、师(旅)炮兵团等,战时要编组各级炮兵群。因此,炮兵战术指挥信息系统不仅要满足炮兵群(团)的作战使用,还要能满足师炮兵的作战使用。在师炮兵作战指挥系统的基础上,精简与炮兵战术指挥无关的功能,增加炮兵群(团)射击指挥功能,以满足炮兵战术指挥控制的需要。

### 2.3.3 炮兵营(连)射击指挥系统

炮兵营(连)射击指挥系统软件功能的改造,应立足于炮兵营连分队战斗指挥的实际需要,在实现射击指挥的基础上,还需开发相应的炮兵分队战术指挥模块,保障分队指挥员实施战术指挥的需要,能显示与分队任务相关的战场信息并实时更新态势,能为指挥员提供实时监控和随时干预所属分队行动的功能,保证能够对所属分队进行有效的指挥控制。

### 2.3.4 炮兵武器平台控制系统

炮兵武器平台控制系统软件功能的改造,应满足快速遂行火力打击任务的需要,使武器数据链(WDL)、公共数据链(CDL)与炮兵武器平台和信息采集设备实现有机融合,能够将侦察设备获取的目标信息数据自动转换为开始诸元,实现从目标信息收集、信息传输到火力打击的一体化。

### 3 炮兵指挥信息系统综合集成应把握的几个问题

#### 3.1 强调指挥信息系统建设的一体化特征，力求整体建设，协调发展

炮兵指挥信息系统综合集成必须注重一体化特征，加强体制建设，从根本上解决标准不统一的问题。按照一体化的要求，建立一套科学实用的综合集成法规体系，作为系统建设的依据，解决技术体制、系统接口等方面标准不一的问题。在整体建设的基础上，科学分工，责权统一，齐抓共管，协调发展，做到主动融入、同步发展，发挥系统的综合优势和智能优势，最终形成一体化的作战体系。

#### 3.2 把握指挥信息系统建设的技术先进性特征，坚持独立自主，积极创新

炮兵指挥信息系统的综合集成，必须紧跟科学技术的发展前沿，离开这个基本的着眼点，对炮兵指挥信息系统的改造都不可能实现真正意义上的一体化。尤其是在现代军事科技飞速发展、日新月异的形势下，更应该坚持独立自主、积极创新，强调把科学技术的进步最先应用到指挥信息系统的建设

和改造上来，这是融入世界新军事变革历史大潮中军队信息化建设的必然趋势和根本要求。

#### 3.3 立足指挥信息系统建设的实战性特征，做到注重实用，提高效益

从着眼实战需要的角度出发，立足现有指挥信息系统和装备，避免重复建设，注重实用，增强系统的综合应用效能；缩短研制周期，加快炮兵指挥信息系统综合集成的进度，提高武器装备的作战效能，使指挥信息系统尽快形成战斗力。以创新的思维，科学的方法，严密的组织，解决好实践中遇到的困难和问题，充分发挥建设资源的使用效益。

#### 3.4 认清指挥信息系统建设的阶段性特征，做好统筹规划，逐步推进

炮兵指挥信息系统综合集成是一项复杂的系统工程，要求高、难度大，涉及范围广，时间跨度大，必须充分认清指挥信息系统建设的阶段性特征，遵循系统开发规律，进行统筹规划，区分层次，明确目标，突出重点，有计划、有步骤地实施。克服随意性和盲目性，把人力、财力、物力集中在可能率先突破、超前发展的关键领域，分步建设，实现滚动发展。

### 参考文献

- [1] 刘钢. 综合信息系统发展概论.北京: 军事科学出版社, 2002
- [2] 赵滨江. 论网络中心战.北京: 解放军出版社, 2004
- [3] 常国岑. 指挥自动化辨析及军队信息化前瞻. 中国军事科学.2005 (1)

### 作者联系方式

通信地址: 河北省宣化炮兵指挥学院战役战术教研室  
邮政编码: 075100  
联系电话: 0313-3366323

# 一种基于智能代理的军事信息系统集成方法

周万宁 孙梅 詹武

**摘 要:** 军事信息系统一体化集成发展是必然趋势。本文针对我军信息系统的应用实际,从信息系统的层次化定义、智能代理的运用方法及集成模式研究三个方面阐述了基于智能代理的信息系统集成思路和实现构想,并对其可行性进行了分析。

**关键词:** 军事信息系统; 层次化; 代理

## 1 引言

现代高科技战争愈来愈依赖于军事信息系统快速、可靠地获取、传输、交换和处理信息。而信息系统的集成有利于信息共享和集中维护管理,使战场控制能力成倍增加。军事信息系统一体化集成所涉及的技术范围广、难度大,我军在该领域的研究尚处于起步阶段,面临的主要问题是各信息系统自成体系,研发缺乏整体规划,各系统层次结构复杂,造成信息系统开放性差、标准化程度低,成为一个个“烟囱”式的信息“孤岛”。单纯的链接、嵌入、附加等生硬集成方法无法将多个系统及其内部元素有机地整合在一体,造成集成后系统部分功能丧失或性能下降。本文根据我军信息系统发展的实际,提出一种基于智能代理的军事信息系统集成方法。信息系统集成智能代理是指以信息系统接入和实现多系统(或系统元素)集成为部署目的的,能够通过预置规则实现其功能的,具有较强适应性和良好交互性的硬软件设备。由于篇幅限制,本文着重从设计思路和使用方法角度,针对基于智能化代理的集成方法中的关键问题展开讨论,并对其可行性进行分析。

## 2 军事信息系统的层次化定义

层次化定义是军事信息系统智能化集成的基础,层次化定义能够为以智能代理为主体的集成方

法提供结构化、标准化和可移植的对象标识和信息传递模式。军事信息系统层次化定义的内容包括对象标识、对象属性定义、信息传输格式定义和数据库组织等内容。由于篇幅限制,本文重点介绍对象标识、对象属性的定义思路与方法。

对军事信息系统的标识,首先必须对其层次划分进行定义。军事信息系统装备一般具备以下层次:集成的系统组-独立系统-子系统-组件(部件)。以军事信息系统“系统组 T”为例,其层次结构图如图 1 所示。由图 1 中可见,军事信息系统对象的描述可采用“树形点分层次法”,即采用“系统组.独立系统.子系统.组件”方法描述。层次标识可采用 1-N 的数字描述,对本级对象的标识以“0”作为结尾。例如“系统组 T 系统 2”的标识为“1.2.0”(系统组 T 编号为 1)。

在定义系统标识的基础上,还可进一步对军事信息系统的属性进行标识,例如:输入输出参数、时间参数、状态参数等。例如,标识号为“1.2.0”的信息系统具有如下表 1 所示的属性定义。可采用“对象标识+属性标识”的方法定义每个对象的属性,因此该系统输出 1 的属性标识为:“1.2.0.2”。

信息系统的结构化定义为智能代理的系统接入、信息引接等功能的实现创造了条件,同时层次化定义明晰了系统内部各层次对象及其属性,突破了系统结构上的限制,使子系统、组件之间的集成成为可能。另外,层次化定义为军事信息系统集成管理及共享数据库的实现提供了信息基础。

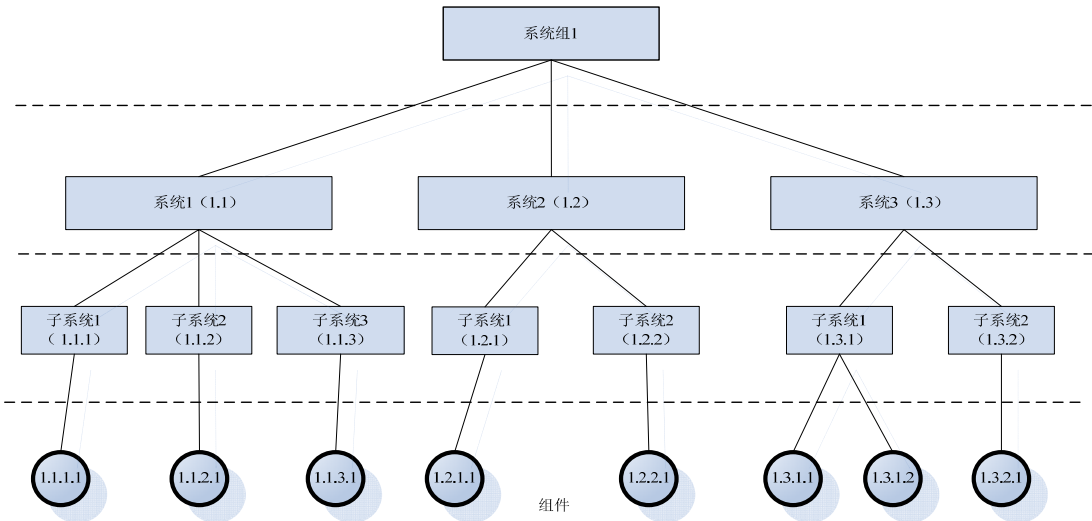


图 1 军事信息系统组 T 的组成层次结构图

表 1 信息系统属性定义示例

名称	内容	属性标识	字符标识
输入 1	数值	1	INPUT
输出 1	数值	2	OUTPUT_1
输出 2	数值	3	OUTPUT_2

### 3 智能代理军事信息系统集成中的运用

我军信息系统集成所面临的最大难题是现有各信息系统的设计、建设和组织运用缺乏统一规范，造成型号多、类型杂、接口各异、开放性差等不利于集成的因素，因此需要采用智能代理技术手段解决现有信息系统的接入和信息引接问题。

#### 3.1 智能代理的功能和组成结构

智能代理在物理上可为软件代理或专门的智能代理设备，既可实现“一对一”的接入也可实现“一对多”的接入，即多个信息系统通过一个智能代理设备接入。在军事信息系统层次化定义的前提下，通过智能代理可实现对系统、系统组甚至子系统、系统组件的集成。智能代理在信息系统集成中的应用示意图如图 2 所示。

智能代理以层次化定义的信息系统为集成服务对象，其基本功能包括：接口功能、信息接入功能及信息预处理功能。接口功能即接口转换功能，提

供多类型接口到标准接口的转换功能，例如：RS232 接口、无线网络接口等到有线网络接口的转换功能。信息接入功能是智能代理通过一定的途径获取或引接信息的能力。信息预处理功能是指智能代理对接入的信息进行过滤、整合、转化等标准化处理，在信息系统层次化标准化定义的基础上形成统一的数据格式和传输报文格式。对于具有关联关系的多个信息系统，智能代理之间还可需要协同调度，实现信息系统的接入管理等功能。

智能代理的组成结构示意图如图 3 所示。

智能代理的组成结构包括信息访问模块、信息传输模块、协同调度模块、信息预处理模块和初始化模块等五个部分。其中，初始化模块实现智能代理的基本配置；信息接入模块是智能代理的主要功能模块，实现信息系统的信息采集和引接功能；信息预处理模块将信息转换成一体化信息平台的统一格式；信息传输模块提供到指定目的系统的信息传输功能；协同调度模块根据一定的调度规则（按最大接入数接入、按级别优先接入等）对多个智能代理之间的行为进行调度，实现系统接入管理等功能。

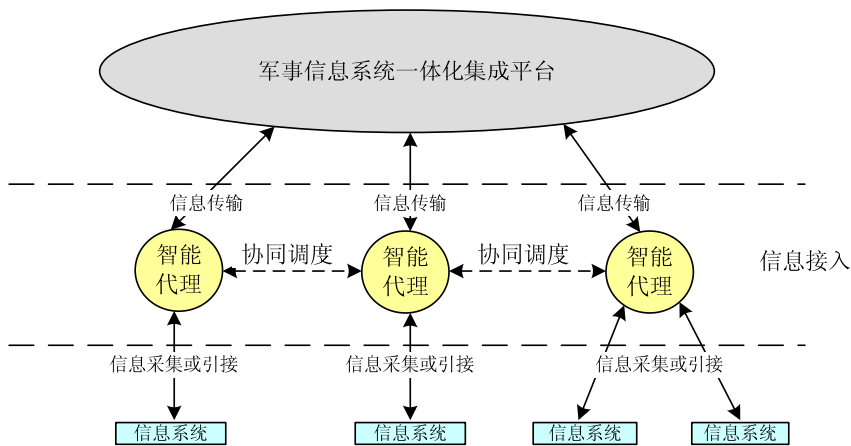


图 2 一体化集成中智能代理的应用示意图

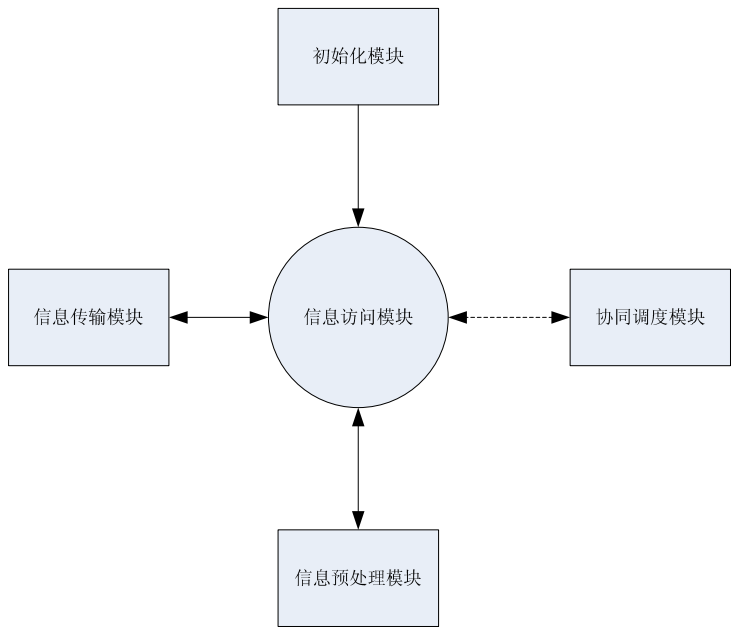


图 3 智能代理的组成结构示意图

### 3.2 信息引接途经

信息引接是智能代理的主要功能，由于我军现有信息系统装备的接口类型多、组织结构各异，因此引接途径有较大差异。

(1) 直接接入

对于具有较好对外接口（如 DDE、OPC、嵌入式接口等）的信息系统，智能代理通过软件接口即可实现信息引接。

(2) 信息采集

对于交互性不好但具有标准化存储结构的信息系统，例如，具有大型开放数据库（oracle、SQLserver 等）支持的信息系统，可直接从数据库

中采集信息；又如大多数通信网络设备和基于 PC 机的电子信息系统均支持简单网管协议（SNMP），可将信息存储到内嵌的标准结构-管理信息库（MIB）中，智能代理可通过 SNMP 协议访问其内部 MIB 实现信息采集。

(3) 间接获取

对于既不具备标准输出接口又不支持标准化存储结构的信息系统装备，可通过其本身具有的控制、维护、管理等系统获取其信息，该方式需要与信息系统装备的设计生产厂家进行技术协调，以实现相关信息的引接。

3.3 智能代理的协作方法

智能代理的一个重要特性是具备协作性，多个智能代理通过特定的通信方式交互信息并在统一的协作调度机制下运行。

知识查询和处理语言（Knowledge Query and Manipulation Language，KQML）语言定义了一套

在代理之间传递信息的标准语法和动作，其特点是对立于特定的通信协议、特定的信息内容和特定的实体，因此 KQML 语言的实现形式非常灵活。智能代理之间通过 KQML 实现通信。图 4 所示为智能代理的 KQML 通信模式。KQML 通信模式为成熟技术，在此不作进一步分析和解释。

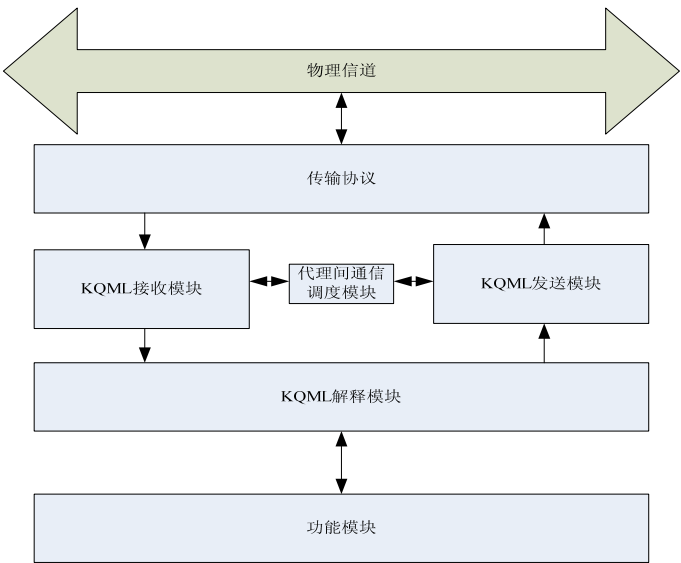


图 4 智能代理间通信模型

军事信息系统的一体化集成中使用的智能代理采用需求驱动的结论共享方式（demand-driven result sharing）实现协作。即智能代理根据需要向其他代理询问相关信息，得到回应后继续进行处理。智能代理间的协作关系通过配置文件中的关系列表明确，在初始化阶段，智能代理的初始化模块分发该关系列表，运行过程中智能代理的协同调度模块维护该表，并根据该表确定通信对象和通信内容。智能代理的关系列表内容如表 2 所示。

表 2 智能代理的关系列表

本地代理标识	远程代理标识	关联参数标识
Agent_A	Agent_B	output
Agent_A	Agent_C	input

4 基于智能代理的集成模式

军事信息系统集成应具有较强的扩展性、适应性和容纳能力。根据接入系统的特点，基于智能代

理的信息系统集成可采用共享集成模式、主从集成模式和综合集成（多层次集成）模式。

4.1 共享集成

共享集成模式下集成的多个信息系统是对等关系，通过建立各信息系统数据库之间的协同关系实现集成。共享集成模式适用于具有独立数据库服务的信息系统之间的集成。共享集成模式的示意图如图 5 所示。

各信息系统原始信息数据库具备同步映射功能，同步保存其他各舰的原始数据副本，当某个信息系统的信息更新后，其他信息系统的对应信息同步发生改变。该集成方式除能扩展一体化信息平台、实现更大范围的信息共享外，还可提供互相备份机制。除数据库同步映射机制外，共享集成还需由各信息系统的智能代理提供一套调度机制，以协调各信息系统接入和信息流转。

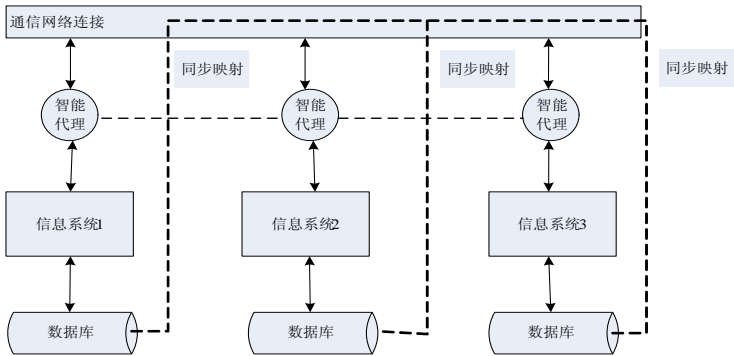


图 5 共享集成模式示意图

4.2 主从集成

主从式集成适用于规模和信息资源不对称的军事信息系统之间的集成。以海军为例，与舰载信息系统相比，岸基信息系统具有部署位置固定、基础设施完善、技术资源丰富、支持维护方便等特点，是“主”系统，舰载信息系统为“从”系统。主从集成模式示意图如图 6 所示。

主从集成模式下，“主”系统与各“从”系统的智能代理机制沟通，获取各“从”系统的信息，

并确定“接入”许可，之后即可建立信息共享等协作关系。军事信息系统的“随遇接入”即可采用基于智能代理的主从集成模式实现。

4.3 综合集成

综合集成是指一体化集成具备“由点到面”的组织能力。以海军为例，舰载信息系统能够按需接入到多个层次的一体化集成平台中，实现更大范围的多层次集成。综合集成示意图如图 7 所示。

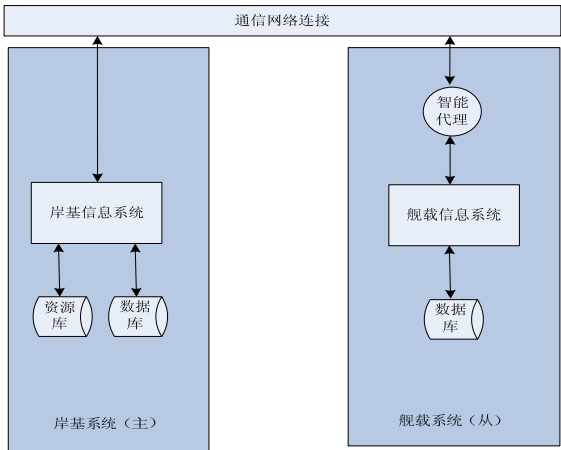


图 6 主从集成示意图

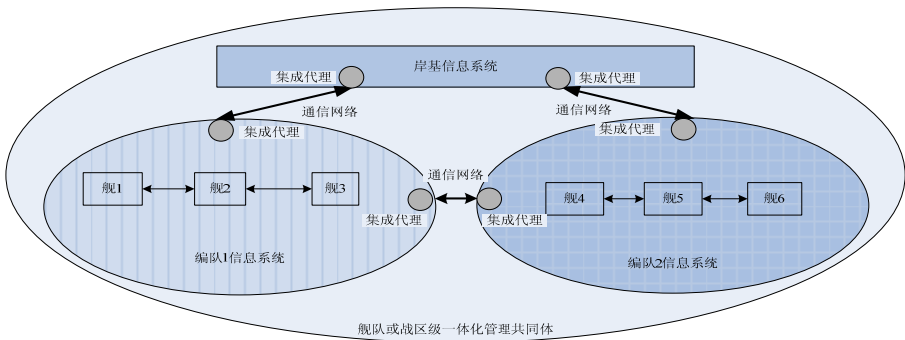


图 7 综合集成示意图

其中独立的舰载信息系统是基本单元，多个独立单元集成为编队级的信息系统的“联合体”，进而多个“联合体”集成为更大范围的军事信息系统“共同体”。

在各“联合体”均具有代表该“联合体”与其他“联合体”通信交互的接口设备，称为“集成代理”。该代理具备独立的数据库结构，记录“联合体”内各单元的基本属性、原始数据属性等数据，同时具备各“联合体”间的信息过滤和数据打包交互能力，综合集成通过“集成代理”间的交互实现了多个“联合体”之间的资源共享，并将管理功能向其他单元和岸基系统的扩展，形成了范围更为广泛的军事信息系统一体化集成管理体系。

## 5 可行性分析与展望

随着现代科技的飞速发展，我军信息系统日趋智能化和小型化，在其复杂程度不断提高的同时，也为其集成化发展提供了广阔的发展空间。例如基于单片机/计算机的特点使智能代理易于部署和移

植。另一方面，各种通信网络在军事信息系统中不断普及，多个独立系统或其内部单元通过网络可形成有机的功能“联合体”，为各种类型的集成创造了条件。例如我军各级各类指挥所局域网络、舰载机载双环网的建设及总线技术（CANBUS）在信息系统装备中普及等都为开展层次化集成奠定了坚实的物质基础。第三，层出不穷的新技术也为基于代理的信息系统集成技术发展提供了有力的支持，例如上述基于 KQML 的代理协作技术，各种对象管理体系结构模型（JMX、WBEM、JINI）、基于 MIB 的对象信息管理技术，分布式数据库同步映射技术、嵌入式开发技术等为各种集成模式的实现提供了全面、多样、可行的解决方案。

在军队信息化建设顶层设计不断深入完善的背景下和装备“两成两力”发展方向的指导下，军事信息系统的体系结构逐步向“横向一体纵向扁平”方向发展，基于智能代理的集成方法为军事信息系统集成提供了新的思路和方法，必将在未来我军信息化建设过程中发挥重要作用。

## 参考文献

- [1] 袁旭梅等. 系统工程导论. 北京：机械工业出版社，2007
- [2] 周苏等. 系统集成与项目管理. 北京：科学出版社，2004
- [3] 叶酉荪. 军事通信网分析与系统集成，2005
- [4] 周萌清. 信息理论基础，航空航天大学，2002
- [5] 王松等译. 网络管理. 北京：清华大学出版社，2003
- [6] 杨苹等. 复杂系统故障诊断综述，测控技术，1998，Vol.17
- [7] Jian-Liang Chen, N.D Rao, A fuzzy expert system for fault diagnosis in electric distribution system, Electrical and Computer Engineering, Canadian conference, 1993 vol 2

## 作者联系方式

通信地址：北京市万寿路3号91655部队计算机应用研究室  
 邮政编码：100036  
 联系电话：010-66974122 13501059410



## 第 3 部分

# 信息安全保障

# 军事信息系统安全问题研究

厉新光 蒋良艳

**摘 要：**军事信息系统安全问题直接关系到能否打赢未来信息化战争。本文从军队信息化建设和军事斗争准备的需求出发，探讨了军事信息系统安全的基本内容，分析了影响军事信息系统安全的主要因素，并重点提出了加强军事信息系统安全建设的措施和对策。

**关键词：**军事信息系统；安全内容；安全措施

## 1 引言

军事信息系统安全是指军事信息在产生、传输、处理和使用过程中保证信息不泄漏，不被冒充，不被修改，不被否认，且保证信息系统不被非授权使用，其功能不丧失。军事信息系统安全是21世纪军事对抗的焦点，是国家安全的重要内容，在国防建设和现代化建设中有着十分重要的作用。随着军队信息化建设的不断深入发展，部队的信息化程度日益提高，加强军事信息系统安全建设成为军队信息化建设和军事斗争准备的关键而紧迫的问题，也是需要高度重视和深入研究的重大课题，它关系到部队在未来作战中能否夺取和保持“制信息权”，并直接关系到未来信息化战争的胜败。面对严重的信息安全威胁，必须采取一系列有力措施，加强军事信息安全保障建设，从根本上提高军事信息系统的安全建设水平。

## 2 军事信息系统安全的基本内容

由于军事信息系统的重要性和易攻击性，使之面临着严峻的安全形势。针对军事信息安全面临的威胁，军事信息安全的内容主要有以下方面：一是实体安全。主要指自然环境和设施安全，如物理设备、位置、物理环境和地域安全因素等。二是通信系统安全。主要包括固定电话安全、移动通信安全和网络邮件安全等。三是电子辐射安全。所有电子设备在工作时都会产生电磁辐射，造成信息泄漏，形成安全隐患。四是计算机安全。主要指计算机硬件系统安全和软件系统安全两部分。五是网络安全。网络安全就是对军事信息网络系统的硬件、软

件及其系统中的数据实施保护，不受偶然的或者恶意的原因而遭到破坏、更改和泄露，系统连续可靠正常地运行，网络服务不中断，以确保军事信息网络系统正常运行。网络安全具体内容包括：第一，逻辑安全。防止网络计算机的黑客入侵，保证军事信息数据的安全。第二，操作系统安全。虽然通用的UNIX等操作系统，都具有一定程度的访问控制、安全内核和系统设计等安全功能。但从国家安全、军事安全的角度考虑，应独立开发使用我国我军自己的安全操作系统。第三，联网安全。主要通过访问控制服务和通信安全服务两个方面来体现，即军用计算机和网络资源不被非授权使用，保证军事数据的保密性、完整性和可信性的军事信息传输。

## 3 影响军事信息系统安全的主要因素

### 3.1 人为因素

人为因素主要是指由于人的主、客观行为对军事信息系统造成的破坏或威胁。主要有以下三方面人员。一是蓄意入侵者。主要是敌对国家的间谍人员和军事信息人员，通过信息网络、电子侦察等各种渠道和手段实施的攻击和破坏。二是黑客闯入。黑客主要采用口令猜测、复制代码、破译密码等方法，通过系统后门进入军事信息系统，实施破坏活动。三是内部人员。主要是指军事信息系统内部的操作人员，滥用职权或超越自己的职权范围，对军事信息系统造成危害。

### 3.2 技术因素

据有关资料估计，安全技术要比信息技术的发

展落后 5~10 年。由于军事信息系统本身在安全方面所存在的脆弱性和种种漏洞,对军事信息系统的安全也造成了潜在的威胁。

### 3.2.1 硬件技术因素

一是电磁泄漏。各种无线电通信设备、微波干线、有线电通信中的架空明线,以及电子计算机在工作时,都会向外辐射电磁波。如计算机控制器以及磁盘(带)机等设备辐射的电磁波,频率一般在 10~1000MHz 范围内。显示器辐射的电磁波象素频率为 10MHz,而行频则为普通电视机的四倍多,达 64kHz。二是电磁波干扰。分为被动式干扰和主动式干扰。被动式干扰是系统内部各种电子设备在工作时辐射的电磁波,在一定区域形成的交叉电磁干扰。军事信息系统中的不少部件,抗干扰能力很差,在干扰电场强度  $E \geq 15V/m$  时,许多芯片就无法工作。主动式干扰是指敌方利用电子干扰武器,对我方实施的有目的的干扰。三是硬件侵入。国外已研制出的微米/纳米机器人可部署到军事信息系统或武器系统附近,它们携带微型传感器窃取信息;细菌炸弹可把芯片细菌投进军事信息系统,嗜食硅片,破坏系统设备。另外,我军现有的绝大多数计算机的主要芯片(如 CPU 和存储器等)是从国外进口的,存在着安全隐患。

### 3.2.2 软件技术因素

一是软件系统自身存在着漏洞。许多系统软件在设计时为方便用户的使用、开发和资源共享,总是留有许多“窗口”,加上设计时不可避免地存在许多不完善或者未发现的漏洞,使攻击者可以利用上述漏洞侵入信息系统。二是软件攻击。计算机病毒攻击就是典型的以软件作为手段的攻击。目前利用软件进行攻击的方式有:数据欺骗(篡改数据或输入假数据)、超级冲杀(用共享程序突破系统防护,窃取数据或破坏数据及系统功能)、异步攻击(将入侵指令掺杂在正常作业程序中,以获取数据文件)、伪造证件(伪造对方人员的磁卡和数字签名等)以及寄生术(用某种方式紧跟拥有特权的用户打入系统)等。可利用的软件武器有逻辑炸弹、陷阱门、特洛伊木马、截取程序、蠕虫程序和其他病毒程序等。

## 3.3 设施因素

军事信息系统的基础设施是全球性的或区域性

的信息系统,主要由通信系统、计算机系统和信息化武器系统组成。这些系统和设施分布在不同的地理空间,贯穿于信息流的整个过程,如果没有严密的安全预防和管理措施,同样会对军事信息系统造成安全威胁,给攻击者以可乘之机。一是运行信息的场所,如信息指挥中心、交换节点、信息化武器阵地和平台等,战时它们首当其冲地成为敌方的重点打击目标。二是处理信息的许多设备难以适应诸如振动、冲击、温度、湿度、灰尘以及电源电压突变等环境因素的影响。三是存储信息的载体,如磁带、磁盘、光盘等,易被敌人得到。四是传输信息的通道易泄密。利用有线信道传输秘密信息,敌方可能会以搭线或在线路上安置感应线圈的方法进行窃听。利用无线信道传输秘密信息,则更难防止被侦听或截获。五是由于军事信息系统的许多网络设施、通信线路是军民共用的,攻击者可以利用与他们联网的地方民用网络,进入军队军事信息系统。

## 4 加强军事信息系统安全建设的措施和对策

### 4.1 强化信息安全意识

一是要从战略的高度认识信息安全的重要性。网络信息系统已渗透到了部队建设的各个层次和方方面面,信息安全将直接影响到国家安全、军队建设和未来战争的胜利。二是要普及信息安全教育。要采取多种形式,大力宣传信息安全保密知识,充分认清信息安全保密的重要性和必要性,自觉把信息安全保密工作作为军事斗争准备和机关正规化建设的一件大事,形成共识。加大管理信息力度,强化对信息系统人员的教育和管理。三是要加强理论研究。围绕打赢高技术条件下局部战争对信息保密的客观要求,着眼信息安全保密的发展,结合我军现代化建设的实际,发动信息管理和使用人员积极研究探讨信息安全保密工作的特点与规律,探索一条符合我军特点的信息安全保密工作路子。

### 4.2 建立健全军事信息系统安全领导机构

加强军事信息安全管理,需要标本兼治,而建立军事信息安全领导机构,则是加强军事信息安全管理之策。从我军信息安全建设实际出发并借鉴外军经验,应在总部统一领导下建立健全军事

信息安全机构。

#### 4.2.1 军事信息系统安全测评与认证中心

其基本职责是依据国家、军队的有关法规和技术标准,对拟进入军队的信息安全保密防护产品(含技术系统)的安全保密性能进行检测、评估和认证;向信息安全产品研制单位提供测评认证技术服务;向有关用户提供相应的技术支持等。对信息安全产品的研制、生产、销售、使用和进出口实行严格有效的控制。

#### 4.2.2 军事信息系统安全研究中心

军事信息安全是一个重大战略性课题,需要专门的机构和人员进行研究。该中心应对信息安全领域进行全方位的研究,创建信息安全学科体系,为军队信息安全建设提供坚实的理论支持。

#### 4.2.3 军事信息网络管理中心

网管中心是目前我军各级单位负责本单位网络管理的业务部门,主要职责是运用技术手段,对我军的各类网络和信息系统进行经常性的巡查、搜索、监测;预防可能出现的安全问题,解决包括物理环境在内的安全隐患。

#### 4.2.4 军事信息系统安全应急反应中心

应按照积极预防、及时发现、快速反应的原则,建立和完善相对独立的应急反应机制。在各大单位组建信息安全专业保障小组;在各级部队、机关、院校和科研机构,建立专业化的信息安全保障力量,增强军事信息系统的防范能力和灾难恢复能力。

### 4.3 做好信息安全保密立法

在依法加强军事信息系统安全保密管理的基础上,还应适应时代的要求,通过立法手段来加强军事信息安全保密管理,并配套出台相应的技术法规,使军事信息安全工作有法可依。我军随着信息化建设步伐的加快,也出台了一些法规,但还很不完善。为此,应加强军事信息安全保密调研工作,抓紧研究制定信息安全保密条例和相关技术性法规,规范我军计算机信息系统的建设和使用,防止信息网络内的军事机密的扩散,保障军事信息的网络系统健康、有序地发展。为了做好军事信息安全

保密的立法和完善有关法规工作,首先,要在《保密法》的基础上,制定军事信息安全保密法规,以利于依法统一管理。其次,要学习和借鉴发达国家在信息安全保密立法方面的成功经验和做法。在充分考虑我军实际情况的基础上,尽量与国际上的有关法规和惯例相接轨。第三,军事信息安全保密是一项技术性极强的工作,在立法和完善法规的同时,还应制定和完善相关的技术法规。

### 4.4 强化信息安全技术研发能力

一是要形成良性的军事信息安全技术研发机制。应将自主研究与使用研究结合起来,形成符合我军实际的良性研发机制。对于军民通用的安全技术和设备,应主要依托国家信息安全产业研发力量,采取公开招标、军品定货等途径解决;对于军队急需而又必须引进的国外先进安全技术和产品,引进后必须进行安全检测并予以技术改造;对于专用的核心技术和装备,要组织军内外专家联合攻关。二是军事信息安全技术研发必须突出重点。当前应力争在以下三种技术上求得突破:第一是能逐步改善军事信息安全状况的、带普遍性的关键技术,如密码技术、病毒防御技术、入侵检测技术等;第二是创新性强、可发挥杠杆作用的突破性技术,如网络侦察技术、信息监测技术、风险管理技术、测试评估技术等;第三是能形成“撒手锏”的关键性技术,如操作系统、密码专用芯片和安全处理器等。三是加强军事信息安全技术研发的规划管理。将军事信息安全设备列入全军装备计划,设立专项经费予以保障,通过军内生产和社会定购等多种渠道,为部队提供系列化的装备保障。

### 4.5 加强军事信息系统安全管理

一是健全规章制度。以实现信息网络安全保密管理的规范化为目标,重点建设秘密信息使用管理、网络管理、密码机使用管理等规定,形成完善的信息网络安全保密管理规章体系。二是要加强网络系统建设的立项把关。在对网络的先进性、适应性、灵活性、易操作性、可扩充性综合把关的同时,突出网络的可靠性、安全性评估,使安全隐患杜绝在立项阶段。三是构建科学合理的防护管理体系。建立信息网络安全管理、监控、密码管理和安全检测中心,负责控制访问权限,防止“黑客”攻

击，对网络运行及上网用户实行监控，实施信息加密。四是建立正规的管理秩序。严格落实各项保密制度，做到各种涉密载体登记清楚，保管严格。采取必要的限制接触措施，从战略级至战术级的信息都要有严格的等级和时限，对接触核心机密的信息人员更要严格把关。五是要综合采取多种加密技术。网络安全的关键技术包括防火墙技术、数据加密技术、安全认证技术等，其中防火墙技术是一种被动式的防卫手段，而加密技术应广泛加以运用。

和军事斗争准备面临的紧迫课题，同时，也是世界各国军队现代化建设的重点目标。近年来，美、俄、印、日等国军队越来越重视信息系统安全，并将之视为赢得 21 世纪军事优势所面临的主要挑战之一。美军强调，要打赢一场信息战，关键在于如何保护自身系统的信息安全。为此，美军建立健全了信息安全管理机构，制定完善了信息系统安全法令法规和标准，开发拓展了一系列信息安全保障技术，并培养了大批信息网络安全方面的专业人才。

## 5 结束语

保障军事信息系统的安全，是我军信息化建设

### 参考文献

- [1] 袁文先. 《军事信息学》. 北京：国防大学出版社，2006.7
- [2] 王正德. 《解读网络中心战》. 北京：国防工业出版社，2005.5

### 作者联系方式

通信地址：江苏徐州工程兵指挥学院

邮政编码：221004

联系电话：0516-83150001

# 基于CORBA的野战指控信息系统安全模型与实现

吕家国 雷武龙

**摘 要:** 本文针对部队野战指控信息系统的应用特点及作战信息存取过程中面临的安全问题, 提出并实现了一种基于野战网络通信平台及 CORBA 技术的 Bell-La Padula 信息安全模型。

**关键词:** 信息系统; 安全模型; 实现

如何在野战指控信息系统中构建可靠的信息安全保障体系, 以解决野战指挥所之间、野战指挥系统与战斗单元之间的信息安全是野战指控信息系统广泛运用并发挥重要作用的关键性问题。目前, 关于野战指控信息系统的信息安全体系研究主要分为两个方面。

1) 野战指挥信息网络平台本身的安全性。它是通过采用多种网络安全设备、硬件及软件加密手段混合使用的方法来保证, 主要包括指挥信息网络加装网络防火墙、通信链路加密机、路由加密机、入侵检测系统以及计算机终端加密等方式。

2) 作战指挥信息数据存取过程的安全性。主要是指指挥信息系统中作战数据信息管理的安全问题, 目前主要通过制定严格的安全策略并采用硬件加密方法来实现。

CORBA (公共对象请求代理体系结构, Common Object Request Broker Architecture) 是由 OMG (对象管理组, Object Manager Group) 组织制订的一种面向对象应用程序体系标准规范, 它的核心是 ORB (对象请求代理, Object Request Broker), 通过 ORB 的软总线机制为解决基于网络的不同硬件平台、不同操作系统、不同程序语言应用系统之间的分布运算与互操作提供了一种完善的解决方案, 适用于构建野战指控信息系统的应用平台。

本文针对野战条件下的作战信息存取安全问题, 提出一种基于野战战术互联网及 CORBA 技术的野战指控信息系统安全模型。

## 1 野战指控信息系统的特点与安全要求

### 1.1 野战指控信息系统特点

野战指控信息系统与固定指控信息系统相比有

着很大的特殊性, 尤其是网络组织及信息的分配, 主要体现在以下几点。

1) 野战指控信息系统的网络平台极为复杂。通常野战指控信息网络 (战术互联网) 根据作战任务及作战地域环境条件而构建, 信道包括短波超短波电台、微波设备 (扩频、无线网桥、卫星等) 及被复线、光缆等, 多种通信方式混合应用使得指控信息系统的网络通信接口极为复杂、网络安全管理非常困难。而且, 在各作战阶段转换过程中, 各种作战要素配置的地形环境、机动路线的变化还随时影响着信息路由及网络拓扑的变化。

2) 野战指控信息系统的应用环境极为特殊。在作战过程中, 上一级指挥所需随时对重点作战方向、重点作战要素、甚至单个作战单元根据作战阶段转换及作战任务需要进行指隶关系转变, 实施越级乃至单兵间的指挥, 呈扁平化指挥方式, 因此作战信息对象边界及作战信息流向的不确定性极大。同时, 各类作战要素 (单元)、战斗终端的使用环境及应用方式不确定, 也造成各信息应用实体高度分散、对作战资源信息应用的范围的不确定性极大。这些都对作战指挥、侦察情报、敌我态势等战场信息的合理有序、实时共享、安全传输带来了很大的困难。

3) 野战指控信息系统软件的安全模式过于简单。

(略)

### 1.2 野战指控信息系统的安全要求

野战指控信息系统的特点决定了其除了面临传统的网络安全问题外, 还对信息本身的安全具有更为严格的特殊要求, 主要体现在以下几个方面。

1) 作战数据库管理系统的安全。作战过程中, 各级指挥所内部的作战数据库服务器都是敌对

方摧毁的重点,除了其数据库内信息的安全保密外,还必须做好作战数据库服务器基于战术互联网的冗余(热)备份工作。

2) 作战信息存取与存储过程中的安全。作战过程中,各类信息应用主体对不同作战信息应用的广度、深度及安全保密程度不同,同时还可能遭受敌对方发起的各种信息攻击行为,因此确保野战指控信息系统内部所有的真实授权用户在作战信息存取与存储过程中的信息安全尤为重要。

3) 作战指挥应用系统本身的安全,即作战指挥控制系统软件的安全,其安全性直接影响着整个野战指控信息系统的信息安全性程度。

要真正解决野战条件下的信息安全防护问题,就必须综合考虑上述因素,在使用相关的网络信息安全硬件设备基础上利用先进的网络分布计算技术,选择并建立相关的信息安全策略与安全模型,才能建立起综合、可靠的野战指控信息系统信息安全体系。

## 2 野战指控信息系统的安全策略与模型

在信息安全领域,为实现安全策略、构建安全模型,往往将与信息相关的实体要素抽象为主体和客体两部分,相关概念定义如下。

主体(Subject)主体是信息的访问和使用者,它包括各作战指挥终端用户、应用程序、进程和线程等,信息主体反映信息的应用及存取行为。

客体(Object)客体是信息及其载体,它主要包括数据表、数据视图、数据文件、磁盘区域以及信息存储的过程等,信息客体反映信息的存储行为。

主客体分离(Subject and Object Apart) 在信息应用和信息安全模型讨论过程中,与信息相关的每个实体要素都只能标识为一种体(即主体或者客体),而且主体和客体之间必须相互独立,只存在单向关系(只能主体访问客体)。

### 2.1 野战指控信息系统的安全策略

军事信息安全的宗旨就是要向合法的服务对象(包括指挥要素、指挥单元、指挥终端)提供准确、实时、可靠的信息服务,而对其他人员,包括

内部、外部的非法访问者及敌对方,不论信息所处的状态是静态的、动态的还是传输过程中,都要保持最大限度的不透明性、不可获取性、不可接触性、不可干扰性、不可破坏性。为此,按照下述要求建立野战指控信息系统的安全策略。

1) 能够为野战指控信息系统定义一个清晰、完整、系统的有限安全规则集。安全策略必须是全局、系统和对所有信息主体普遍适用的规则,对信息系统中已经识别的主/客体,系统才可以根据一定的安全规则来决定某个主体能否存取特定客体。系统的安全管理员能够对整个应用系统的安全模型及系统结构进行维护、修改等,而数据库管理员只能对作战信息数据库中的数据进行维护和管理。

2) 能够为系统中的每个客体指派相关的存取控制和认证标识。通过建立安全策略为信息客体的每个对象加上安全级别标记,区分客体的安全敏感度层次以及可能存取该客体的主体存在模式,同时也用来确定不同用户允许存取的信息安全界限,这一界限的解释必须和安全策略中的规则相一致。

3) 能够为系统应用中的每个信息客户进行标识,并通过用户标识来区分不同类别的用户。野战指控信息系统能够利用模型协调、管理得到授权并已标识的用户,能够对信息主体存取的信息类型进行授权验证,同时能够安全地保存和维护这些标识和授权信息。

### 2.2 野战指控信息系统的安全模型

贝尔—拉帕丢拉(Bell-La Padula)模型是一种成熟的强制型安全模型,它通过信息主体(用户以及代表用户的应用程序和进程)必须面对的“存取限制矩阵”来确保信息的安全,通过区分信息主体的安全级别、客体的敏感度层次以及利用相应的安全规则集合来增强系统应用的安全性,与其他安全模型相比,更加适合于构建野战指控信息系统的安全结构体系。模型具有以下特点。

1) 模型基于系统元素的密级而建立,密级用安全级别表示,每一安全级别(Security Level)均由密级(Secret class)和范围(Catagories)组成,记为  $L = (S, C)$ 。密级集合包括 4 个元素{绝密、机密、秘密和公开},范围集合依赖于系统元素所依赖的环境和应用领域,如{潜艇部队、导弹部队、师、团}。由此可得到安全级别的部分实例,如(绝密,潜艇部队)、(机密,行动方案)

等。

2) 各种信息元素安全级别的集合可以具备一定的支配关系, 设  $L1 = (S1, C1)$ ,  $L2 = (S2, C2)$ 。要使  $L1$  支配  $L2$  只有: ①  $S1 \geq S2$ , ②  $C1 \supseteq C2$ , 标记为  $L1 \geq L2$ 。

3) 模型中主体的安全级别表示了信息用户或应用程序进程的存取权限; 而客体的安全级别则反映了客体信息的敏感度, 也反映了未经授权向不允许存取该信息的用户泄露此信息可能造成的潜在危害度。信息客体的建立者拥有对客体的所有权限, 并可以将这些权限(客体之间的隶属关系除外)授予其他用户或从其他用户收回权限。

4) 模型中主体对客体可执行的存取方式包括: 读取(Read)、添加(Write)、执行(Execute, 对程序及进程而言)、编辑(Modify)。

5) 模型共定义了 8 种与系统状态相关的信息操作: 取得访问权限(Get Access)、释放访问权限(Release Access)、赋予访问权限(Give Access)、收回访问权限(Rescind Access)、激活对象状态(Create Object)、取消激活状态>Delete Object)、改变主体安全级别(Change Subject Security Level)、改变客体安全级别(Change Object Security Level)。

6) 为进一步确保系统的信息存取安全, 模型还规定了一组系统工作中必须满足的安全规则:

- No read-up secrecy: 一个主体仅能读取安全级别受此主体安全级别支配的客体信息;
- No write-down secrecy: 一个主体仅能向安全级别支配此主体安全级别的客体写信息;
- Discretionary Security: 一个主体只能在获取了所需的授权后才能进行相应的存取操作;
- Non-accessibility of Inactive Objects: 一个主体不能读取一个未激活客体的内容;
- Rewriting of Inactive Objects: 每个新激活客体均被赋予独立于前一次激活时的初始状态。

这些规则集有效地控制了系统中信息的流动方向及操作需求, 既能够防止高安全级别的信息流入低安全级别的客体, 又保证了低安全级的信息主体不能存取高安全级别的客体信息。

### 3 野战指控信息系统安全体系构建方法

基于 CORBA 的分布对象技术采用面向对象的多层客户/服务器计算模型, 将分布在网络上的所有资源都按照对象的概念进行组织: 每个对象都有定义明晰的访问与调用接口; 创建和维护对象实体的应用程序统称为服务器, 而按照对象接口访问与调用对象实体的应用程序都称为客户; 服务器中的对象不仅能够被访问, 而且其自身也可以作为其他对象的客户。在基于 TCP/IP 协议的通信网络中, 对象请求代理 ORB(Object Request Broker)像一条数据通信软总线把分布式系统中的各类对象和应用连接成相互作用的整体, 从而实现各对象之间的互操作。

野战条件下各种信息主体要素在作战地幅内高度分散, 作战过程中各级指挥所、作战要素、作战单元与战斗模块之间只能依托野战指挥信息网络互联互通。野战指挥信息网络是依托被复线、光缆、短波超短波电台、微波设备及卫星通信等信道组建的野战战术互联网, 且各种通信信道综合使用、互为备份。

野战指控信息系统的安全模型基于战术互联网与 CORBA 技术构建, 可从根本上解决野战条件下信息要素层次多、配置地域广且安全保密要求高的问题。

模型的系统应用结构图如图 1 所示。

系统工作流程如下。

1) 基本指挥所信息中心的应用服务器及备份应用服务器向身份认证与对象管理服务器申请注册, 注册后各应用服务器相互交换数据库服务器的对象引用信息, 每个应用服务器就可同时管理本地及备份的数据库服务器系统。

2) 各作战要素及战斗终端向身份认证及对象管理服务器申请身份标识并注册。

3) 身份认证及对象管理服务器的安全管理员根据作战阶段及作战任务情况向作战要素及战斗终端按照身份标识的不同进行安全等级授权, 并发给相应的应用服务器对象引用信息。

4) 身份认证及对象管理服务器向应用服务器激活已经注册的作战要素及战斗终端标识与安全等级, 应用服务器就允许已经授权并激活的用户终端访问。



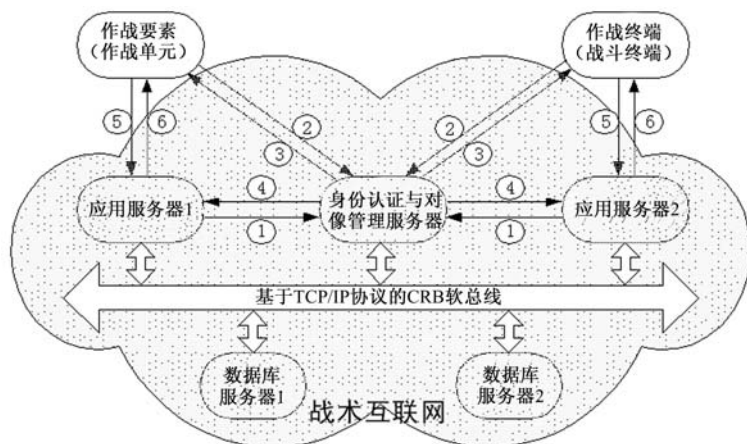


图1 模型系统结构图

5) 作战要素和战斗终端向应用服务器发送信息存取请求，应用服务器对其发来的信息存取请求进行安全规则匹配，匹配成功则与数据库之间进行信息存取处理，不成功则丢弃信息存取请求。

6) 应用服务器向作战要素与战斗模块返回其信息请求的处理结果。

7) 各作战要素及战斗模块之间的协同动作及信息共享在通过认证服务器的身份认证并授权后方可进行。

8) 身份认证及对象管理服务器的安全管理员可根据作战阶段转换及作战任务转变要求对作战要素及战斗终端的身份标识及安全等级授权进行改变，同时向应用服务器激活相应作战要素及战斗终端的新的身份标识及安全等级。

模型结构特点如下。

1) 通过各指挥所之间的服务器冗余备份手段确保了各种作战信息的存储安全。不同数据库服务器基于野战战术互联网在作战地幅范围内异地配置，应用服务器保证了数据库内容版本的一致性。

2) 野战指控信息系统的安全模型工作于作战指挥过程的所有阶段。应用服务器内部集成了作战要素身份认证、安全规则集定义、客户访问请求处理、数据库管理、访问监视器等功能模块，应用服务器内部的安全级别逻辑分层确保了信息数据的存

取安全。

3) 所有作战要素（指挥所及携行指挥终端设备）及战斗模块均为处于同一应用层次的对象访问实体。

4) 各级指挥所的指挥终端、身份认证及对象管理服务器、作战要素、战斗模块均可依托野战战术互联网通过 ORB 软总线进行接口调用，有效地消除了现有野战指控系统与武器系统不同硬件平台、不同操作系统、不同应用系统之间的差异，能够实现各类作战信息共享与系统之间的互操作。

构建野战指控信息系统安全模型是一项复杂的系统工程，还面临如下两个方面的关键性问题。

#### (1) 信息主体与客体的安全层次分级问题

作战过程中对各类指挥要素、作战要素（单元）、战斗单元与作战信息的安全层次合理分级非常重要，尤其是在不同的作战阶段转换过程中如何快速、合理地根据作战指挥需要更改信息主体与客体的安全层次等级及信息主体、客体之间的隶属关系，需深入探讨。

#### (2) 野战战术互联网的通信协议一致性问题

野战条件下，数据通信网络通常综合利用有线、短波超短波电台、微波设备、卫星等通信手段，如何保证野战战术互联网中通信协议的一致性与网络信道的可靠性需进一步深入研究。

### 参考文献

- [1] 刘启原, 刘怡著. 《数据库与信息系统的的海》. 北京: 科学出版社, 2001 年
- [2] 朱勤. 数据库安全技术, <http://tech.csai.cn>

### 作者联系方式

通信地址: 河北保定市 66393 部队 401 试验站 邮政编码: 071000 联系电话: 0312-5980686

# 作战指挥系统信息安全体系结构的思考

苗小伟 李殿伟

**摘 要：**作战指挥系统信息安全体系结构的设计必须以作战指挥的安全需求为牵引，以密码芯片（模块）为支撑，在网络结构中嵌入密码基础设施，通过电子密钥管理系统提供的端到端的互操作能力；将网络安全服务向作战指挥软件体系延伸，构建海军作战指挥应用软件体系；通过信息资源的认证服务和目录服务，构建信息资源控制的信任体系和可信的作战指挥系统；实现基于信息系统整体运用的信息安全体系结构。以安全服务为平台，通过策略服务，实现安全操作、管理、应用在作战指挥体系结构内的融合；实现包括网络体系结构、软件体系结构和信息资源部署体系结构在内的海军指挥信息系统的整体协调运用。

**关键词：**作战指挥；信息安全；指挥信息系统

指挥信息系统安全体系结构的设计，要以作战指挥安全需求为牵引，将人、武器装备、数据库等作战指挥要素融入到以网络为中心的闭环系统之中，确保信息资源在安全的构架下，进行作战指挥应用、安全服务和网络管理上的融合，建立面向服务的指挥信息系统整体运用的安全框架，实现信息流对物质流和能量流的安全有效控制。

## 1 海军作战指挥的安全需求

在作战指挥中使用信息的目的是支持决策，因为任何信息系统的最终度量指标是所得出的决策质量和时机。如图 1 所示：决策的信息支持分两个阶段。首先是战场感知，为做出决策提供准备和支持。目标是指挥员能够很容易地搜索到信息并把信息提取出来；其次是指挥控制，决策的本身是把信息传递给相应的部队，并得到正确地执行。其安全需求是以网络服务的形式，为整个决策过程提供无缝隙的、可靠的信息质量保障，网络服务的核心就是信息安全的服务。

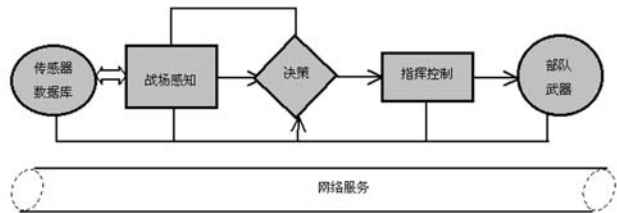


图 1 指挥决策中的安全需求

### （1）战场感知

战场感知是贯穿整个决策过程的信息活动，要实现信息的高质量保障，其安全需求是将安全机制嵌入到传感器、数据库、武器装备的前端，使其信息一经产生就受到保护，并贯穿到信息收集、信息处理、信息显示的全过程。

1) 信息收集。信息收集是根据作战指挥员的需要，对情报、监视、侦察和综合保障的数据进行采集。需要保护的信息一经产生，便按照整个大系统统一的标准、统一的策略安全存贮、控制和分发，将物理空间上广泛分布的数据收集体系虚拟为可视化、操作性强的本地数据中心。这种安全的虚拟数据中心便于作战指挥数据库信息的源源不断的采集更新、专业化维护，为指挥决策提供近实时的后台信息支持。

2) 信息处理。信息处理从海量探测信息中进行提取、融合和汇总，形成统一的战场态势。要实现信息在一个较大范围的自动提取、自动融合、自动汇总，减少人工干预，许多信息并不一定是保密的，但为有价值的信息提供安全保障，为信息系统提供快速、准确、自动的鉴别能力。同时，只对受保护的信息进行处理，可以防御拒绝服务、流量分析和错误信息插入、屏蔽掉大部分冗余信息的干扰，提高信息的可信度和自动化处理能力。对于任何信息对象，都要有一个敌方不能识别，而己方可以识别的标识描述它是什么、来源和属性情况，没有这种标识或标识不可信，信息本身很难直接综合或使用。对信息处理流程的设计必须包含对各种标

识进行鉴别、对信息流进行保护、按策略进行流向控制等。特别是未来动态多用户信息融合、动态数据库自动维护方面,还应包括对信息的环境属性标识(如时间戳、资源大小、范围)、过程属性标识等提出可信和可靠性需求。

3) 信息展示。“可视化”决策是指位于作战指挥链各个决策位置的指挥员对自己指挥的各个要素之间的逻辑关系、信息交互矩阵等以易于理解的图形方式输出。信息展示并非是简单的信息显示,而是一个复杂的人工干预、信息反馈和网络认知的过程,通过提供各类标准化密码中间件供作战软件设计人员调用,使信息在存贮、查询、检索的过程中得到透明的安全保障。

#### (2) 指挥控制

作战指挥控制是作战力量运用时的信息活动,指挥控制强调的是:一旦做出决策,必须将首长的决心传达到相应的作战单元,信息系统应能适应快速变化的作战进程,在必要时作出修改和调整,通过信息流对物质流和能量流进行控制。

1) 信息分发能力。信息分发应能满足指挥员更大的指挥分散性,更大的集中度和最低限度的密码通信能力。指挥分散性是强调作战人员的自主搜索获得信息。不同的作战人员对态势的采用方法不同,密码保障要能从规则、策略、权限等方面进行定义,满足不同人员对信息的需求。集中度是满足指挥员对信息传播的某种程度的控制需求,密钥由顶层逐级向下分发,发方控制收方的特点,可以满足指挥员逐级、越级、接替和协同指挥的需求;最低限度是指在最恶劣的环境下,也必须有密码通信保障的能力。

2) 信息控制和反馈能力。在作战指挥控制过程中,对战场监视、侦察、控制和战斗效果评估能力及向决策环节的反馈能力,依赖开发持续发挥作用的综合感应、组织计划和指挥控制的系统。

3) 信息配置与变更能力。海军作战指挥要向以网络为中心的方向转型,其中一个非常重要的方面是信息系统能够快速适应战场的变化,以便确定支持作战的要素的快速定向和重定向功能,在高速紧张的战术情况下,能够采用自动化过程简化人工决策来缩短决策周期。目前海军作战任务和指挥机构的变化仍然基于物理上的通道、线路、电路分配、按区域的通信组织管理。快速的信息配置与变更的能力,要求海军作战软件系统通过密码基础设

施的策略服务,对密码进行适时配置和变更,改变了密码配置便改变了指挥关系和指挥域,底层网络、通信、链路的配置则是随着应用层的改变而自动改变。

## 2 信息安全的硬件体系结构

在网络体系结构中嵌入安全体系结构,就是从终端安全体系结构开始、为系统安全体系结构扩展到作战应用的安全体系结构提供硬件支撑。

#### (1) 终端安全环境

目前国内外研究的可信计算主要是解决终端计算环境的安全。基本思路是将自主知识产权的密码模块作为可信根嵌入信息装备的端节点,运用多层密钥保护和综合安全机制,对作战指挥数据和作战应用软件进行保护和隔离,从物理特性上提高网络管理的安全性、信息分发的保密性和信息资源的可控性。

#### (2) 网络安全管理

安全管理中心是集综合预警、应急响应于一体的重要基础设施,以网络的安全运行和物理边界防护为目标,对网络实体进行认证、对网络运行进行监测和网络行为进行审计、对网络接入和信息流向进行控制、对网络管理信息进行备份和系统恢复。实现信息系统逻辑要素的“实体”、“通道”、“配置”接口在物理操作上的真实、可靠、连续性。

#### (3) 信息安全管理

密码管理中心是集密码管理、密钥分发、密码服务于一体的重要基础设施,以数据的安全保密和逻辑边界防护为目标。电子密钥管理系统(KMI)为所有的端节点提供端到端的保密通信能力;公钥基础设施(PKI)为所有的信息资源要素提供分布式标识注册系统,提供资源定位能力。密码分割提供高效域间管理能力。按指挥关系、使命任务、业务管理、风险等因素划分不同的信息保护的逻辑域,建立不同的虚拟逻辑网,域内实现高效的保密通信,域间实现协商的保密通信,在全军范围内形成纵向到底、横向到边的保密通信逻辑框架,实现三军协同指挥和联合指挥。

## 3 作战指挥软件体系结构

作战指挥软件的安全、可靠、可控性设计,依

赖于自主知识产权的底层加密算法的安全、正确实现和有力保障,即通过密码保障来控制系统内的信息移动、信息访问权限,由于作战应用数据目前没有实现有效的逻辑隔离,还难以实现高安全级的控制。

#### (1) 作战应用数据与操作系统之间的逻辑隔离

许多作战软件系统都是在操作系统上开发出来的。一般来说,计算机硬件运行正确,其完整性源自对硬件开发者的信任;操作系统运行正确,其完整性源自对软件开发者的信任,这两点我们都受制于人。虽然操作系统提供了基本的数据隔离机制,显然不可能满足指挥信息系统安全的需求。首先,操作系统不能满足基本的专用军事安全策略的要求(能满足也不敢使用),还存在一个“应用程序空间”,直接在物理和操作系统层面对重要军事信息进行“明信息”操作,应用软件发送、存储、检索或修改重要信息时都存在安全缝隙;其次,操作系统允许特权软件绕过操作系统的限制,留有后门隐患。软件的设计和使用人员难以确保应用程序所使用的数据处于独占状态,攻击者可以通过操作系统及更底层的数据操作来获取应用程序所使用的数据。

#### (2) 多种信息级别之间的逻辑隔离

即使是保密终端,目前的密码管理基本都是简化的密钥管理方案,实现粗颗粒的保密控制,尚不能实现不同密级同时通信中多种信息级别的应用数据之间的逻辑隔离。多级安全是作战软件体系结构设计上的一大挑战,一个指挥员,特别是中间级指挥员,可能在不同的作战编成中担任不同的角色,目前一个方案一套装备,一个角色一个身份卡的现象还很普遍,难以做到同一平台上不同用户群之间的逻辑隔离,特别是动态的创建、撤销这样的基于任务的用户群。

#### (3) 信息安全服务接口

由于目前作战应用软件的开发大多在商用平台、通用操作系统和协议上进行开发,密码保障仅作为独立的子系统为作战指挥提供有限的支撑,安全机制与安全服务等难以向作战指挥软件体系结构中延伸。密码中间件为网络安全服务向作战指挥软件体系延伸提供安全接口,如:对称加密与解密、非对称加密与解密、信息摘要、单向散列、数字签名、签名验证、证书认证,以及密钥生成、存储、销毁等服务向具体的应用领域延伸,进而形成系统

安全服务接口、应用安全服务接口、储存安全服务接口和通信安全服务接口。安全中间件可以跨平台操作,为不同的作战应用软件集成提供方便,满足用户对系统伸缩性和可扩展性的需求。密码中间件与作战指挥功能中间件集成,使设计开发人员无须涉及敏感的密码领域就能够构造高安全性的作战应用,使用人员在不知不觉中透明地获得高质量的安全保障。

## 4 作战指挥信息资源管理的体系结构

信息资源特别是要素资源,如指挥机构、指挥人员、数据库、武器、传感器等,以什么样的体系结构集聚在互相连接的计算机系统周围,形成网络空间闭环的作战指挥系统,是一个资源管理的战略问题。运用公钥基础设施建立标识认证体系实现信息资源管理,虽然已经逐步形成共识,但在整体体系结构的设计、资源利用等方面还有很大差距。

#### (1) 建立信息资源标识体系

信息资源通过公钥基础设施注册的形式嵌入信息系统,是为了作战人员快速发现、定位和验证资源,从而实现可信信息交互。进行信息资源管理,是构建网络空间作战指挥系统的基础性安全工作。首先,任何实体无论规模大小、范围多大、来自何方都应有相应的标识。

**标识分类。**从作战指挥来看,包括信息系统、武器装备、指战员、知识库、综合保障等海军作战指挥要素都可以密码标识的形式嵌入密码基础设施,信息资源的管理就转化为单一的标识(证书)管理。实体的分类是具有惟一性和独立性的标识集合。如用户标识、地址标识、号码标识等互为独立、互不渗透的标识空间就称为类。

**标识分级。**当某一类实体标识空间庞大、地理分布广泛,可以按地域、编制体制等分级管理,这种相同类中不同的管理层次称为级。

**标识认证。**标识认证是以数字签名技术实现的。签名可以分成:单位级签名,用户级签名,实体级签名,对标识的证明和对数据的证明表现形式相同,但证明的对象不同,标识认证证明标识的真伪,而数据认证则证明数据的真伪。

#### (2) 建立海军指挥信息系统信任体系

信任体系是运用电子签名的方法对一个信息的

主体身份, 实体标识、内容真伪进行准确的验证, 便于资源的定位、验证的相互关联的整体。

1) 基于身份的认证。人作为作战指挥的第一要素, 证书代表用户身份, 用户证书是标识的一个关键性的子集。判断一个信息是不是来自某一个指挥员, 不是看这个信息来自哪个指挥平台, 而是验证信息中是否包含这个指挥员的标识, 作战指挥人员有了权威统一的逻辑身份, 可以实现快速身份定位, 不需要通过电话等其他网外手段的验证。指挥员可以突破物理位置的限制, 在任何平台实施灵活的作战指挥, 同时对作战指挥人员在网络空间的行为可以进行审计、监测、仲裁。

2) 基于装备的认证。在武器装备中嵌入密码组件(芯片), 就可以为其建立标识和分发密钥, 就能把该装备的属性发布给授权的网络实体而不是暴露给未授权实体或敌人。武器装备的认证也是标识认证的一大子集, 在作战指挥信息系统中资源管理和定位中起到至关重要的作用: 了解什么样的设备时刻连接在网络上; 该装备的存储、显示、输入/输出能力和位置等终端装备的能力; 状态和准备就绪情况; 确保入网的信息装备都是经过认证的。

3) 基于信息流程的认证。在网络空间作战指挥系统的信息交互中, 不仅存在指挥员之间在用户层的关联关系、指挥员与装备的关联关系, 还存在装备与装备之间的关联关系。作战指挥信息在其完整的信息流程中, 可能穿越不同的网络环境和计算环境, 基于信息流程的认证也可以细分为通信标识认证和进程标识认证等。

### (3) 建立作战指挥体系

网络空间的指挥体系就是指挥要素之间的关联关系, 将现实空间的海洋作战指挥要素映射到网络空间, 将无界的标识空间到无界的公钥空间的复杂映射, 转换为有界标识空间到有界公钥空间的简捷映射, 在网络空间形成海洋各类指挥要素纵横联系的有机整体。标识(证书)代表各个指挥要素, 具有可替代性和可扩展性, 逻辑上与部队体制编制关联, 物理上与该节点的地理位置和具体的装备平台分离, 通过标识服务和目录服务, 建立一个相对稳定的以网络为中心的作战指挥体系。

建立一套网络空间与现实空间相对应的指挥机构和指挥人员的标识体系, 并确保网络空间标识的唯一性、可信性和可证明性;

建立一套作战指挥的规则集合来维护网络空间

秩序, 实现作战指挥要素按指挥关系、指挥规则相互关联;

建立一套策略机制来适应战场指挥节奏的快速变化并适时作出逻辑上的调整而不是物理上(信息系统物理配置)的调整。

## 5 信息系统整体运用

当指挥信息系统的终端装备中嵌入了一颗“中国芯”, 网络结构中嵌入密码管理中心, 作战应用软件中嵌入了信息安全接口, 信息资源以统一的安全体系结构进行部署时, 就可以实现基于整体运用的信息安全体系结构。

### (1) 面向对象的远程控制架构

通过远程电子密钥分发和密钥配置, 战术上可以对所有节点进行分割、组合和动态编成, 技术上可以实现基于对象的精确认证、重新定义和多级安全。

**精确认证。**建立指挥人员身份, 确保其网络身份的惟一性和可靠性, 识别指挥员是验证一个信息流中是否包含该指挥员的身份信息, 而不是验证信息来自哪个平台或专用装备, 更不是通过电话等其他方式进行识别; 装备中的密码芯片(模块)实行严格统一研发管理, 芯片嵌入统一的防伪标识和算法, 所有入网的密码芯片(模块)均可在统一的策略下, 得到可靠的监控。

**重新定义。**通过人工密钥配置或远程密钥人分发, 允许在不同的密级上对设备的再定义。平时信息装备仅携带一个可信根(初始密码), 可以是无密级的敏感设备。一旦确定了信息装备的使用者和网络环境, 再对密码进行重新配置, 分发相应的密钥, 配置该装备所必需的信息资源, 快速定位。重新定位不危及该设备的原使用者、高密级或核心通信的安全。

**多级安全。**通过密码模块/芯片的动态可编程, 将不同级别的算法和密钥加载到同一芯片中, 在同一密码机(密码组件)中实现不同密级和不同级别网络间的互操作。一个模块/芯片上可实现多用户同时通信、不同密级的用户同时通信、不同网络间同时通信、不同信号同时加/解密, 用密码逻辑分隔, 互不干扰, 用户之间不能通过错误恢复、密钥恢复和其他环节导出其他用户的信息, 一台装备可以划分多个不同等级和密级的逻辑区域, 一个

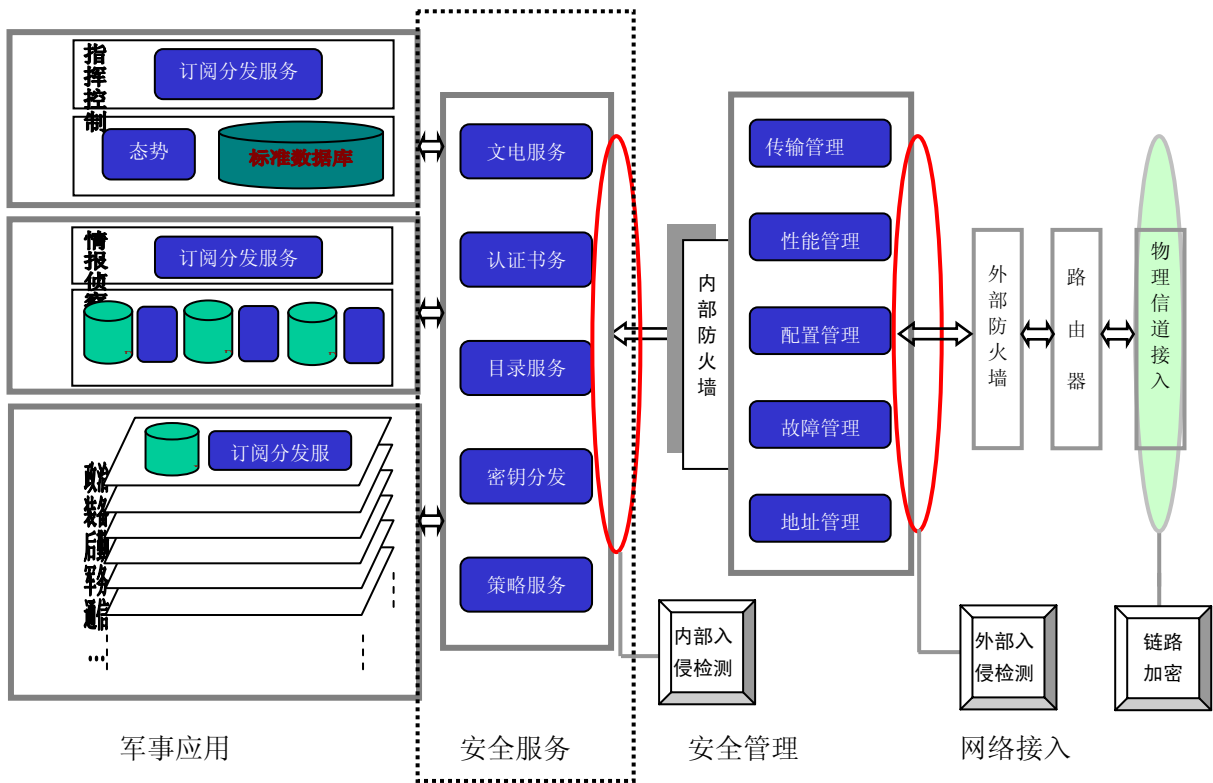


图 2 面向服务的平台架构

指挥员不必使用多台装备，也不必使用多张身份卡与不同等级的用户通信，实现单机多级信息安全。

(2) 面向服务的信息管理架构

如图示 2 中虚线所示，在作战指挥应用与网络管理之间形成面向服务的平台架构：以密码基础设施为依托，对系统中安全部件实施综合监控与管理，使通用的安全服务向千差万别应用领域、特殊环节延伸，构建面向服务的海军指挥信息系统整体运用的架构。

**文电服务。**密码电报提供与指挥员意图相一致的端对端的核心文电服务，满足指挥员对信息控制的集中度需求；安全 Web 服务为所有的信息发布者提供向广泛分布的作战要素通告、发布和分配信息的保密手段，满足指挥的分散性需求，广泛适用于办公自动化和装备、勤务保障。

**认证服务。**认证服务提供了分布式系统中的资源标识的创建、撤销、认证和授权支持，通过协调各个分布的安全系统提供统一的签名功能，可以用来透明地横跨底层系统为作战指挥提供信任认证功能。这种信任关系的扩展，就是通过一个分布式、结构化的证书管理系统来建立一个可信的网络资源

要素的关联体系。

**目录服务。**通过一个结构化的命名服务，提供在分布环境中资源定位和管理资源的能力。目录提供分布式信息服务中所表示的所有客体的访问控制。提供信息的多个元素与特殊的人或设备的关联的方式，允许应用查看或发现分布的资源。

**密钥分发服务。**以电子密钥管理系统为支撑，提供与指挥员的意图相一致的端对端信息管理能力。密钥分发不仅是整个作战体系结构安全的核心，也是控制的核心，密钥分发能力决定了端到端的互操作能力，动态创建和撤销协同通信的逻辑域和逻辑通道的能力，是保密通信、构建指挥关系、实现虚拟作战编成，建立网络化作战指挥体系核心支柱。

**策略服务。**密码基础设施（KMI/PKI）管理除了为自身提供更高级别的安全管理外，更具发展前途的是它的策略的创建和管理服务，将是海军作战指挥向以网络为中心转型的中枢神经。首先，提出一种基于信息资源管理规则的策略描述语言，不管底层网络结构如何，而是对整个战场的指挥规则、控制策略、逻辑通道、信息交换关系等，用一种策

略语言来描述安全规则。其次，建立作战指挥策略库。将作战指挥中信息控制、资源共享、条令条例、指挥规则等信息控制模型进行抽象，建立作战指挥策略库，并可以随时生成、查询、审计策略报表。最后，通过可视的安全体系拓扑结构，安全策略的一致性协调对信息资源的配置进行统一管理和安全分发，定义符合指挥员需求的统一信息控制规则、策略，根据战场情况的变化进行逻辑上的调整，而不是物理上的调整。使整个作战指挥网络在功能和效力上协调统一，建立信息系统整体运用的策略控制体系。

个融合的过程表现为信息系统综合集成由装备集成、系统集成、体系集成到力量集成，安全体系结构本质上是一个可重构的逻辑体系结构，是从可信计算到可信网络，从可信网络到可信应用的整体体系结构。构造作战指挥系统的逻辑基础是自主可控的密码技术，而不是标准协议。可重构的特性是指在作战指挥层面，通过密码芯片的动态编程、密钥人工注入、远程分发，实现对作战指挥要素、指挥域、指挥规则进行逻辑上的快速调整。实践表明，任何在信息安全体系结构上忽略密码技术核心地位的设计都是会走弯路的。

## 6 结束语

信息系统整体运用的概念是个融合的概念。这

### 参考文献

- [1] 《海军信息系统组织运用机制研究》. 海军指挥学院. 2005 年
- [2] 《海军网络中心战》. 海军装备部电子部翻译出版. 2005 年
- [3] 《信息保障技术框架》(3.0 版) 北京中软电子出版社. 2002 年 3 月
- [4] “信息安全方向与优先项目”. 南相浩《信息安全与通信保密》2006.11 期

### 作者联系方式

通信地址：北京市西三环中路 19 号-33

邮政编码：100841

联系电话：010-66969106      010-66969116



# 军用计算机信息网络系统信息安全对策浅析

陈松德

**摘 要:** 在新军事变革的浪潮中,随着我军信息化建设步伐的不断加快,计算机信息技术在部队的应用日晶益广泛。由于信息网络的开放性问题,使得我军的信息网络的信息安全还存在很多问题,网络安全工作明显滞后于信息网络建设的步伐。本文将针对当前我军信息网络安全中存在的诸多问题,从网络安全技术及网络安全管理两方面提出相应的解决对策。

**关键词:** 信息化建设; 计算机网络安全; 信息安全; 对策

随着全球信息化建设的快速推进,网络中接入信息基础设施的数量不断增加,信息系统软件建设水平日益提高和完善,计算机网络信息的安全问题变得日益突出和重要,根据US- CERT<sup>1</sup> 组织的统计,从1998年到2002年期间,该组织登记网络安全事故的数量增长率超过50%。根据国家信息安全报告课题组编写的《国家信息安全报告》,如果将信息安全分为9个等级,我国的安全等级为5.5,安全形势十分严峻。与此同时,我军各种信息网络的的信息安全问题也同样不容乐观。

## 1 我军计算机信息网络信息安全存在的不足

### 1.1 缺乏自主的计算机信息网络软件和硬件核心技术

我国信息化建设缺乏自主的核心技术支撑,计算机网络的主要软、硬件,如CPU芯片、操作系统和数据库大多依赖进口,如我军信息设备的核心部分CPU大多由美国和我国台湾地区的生产商制造,我军计算机网络中普遍使用的操作系统则基本上全部来自国外,这使得我军的信息网络系统都存在大量的安全漏洞,极易留下嵌入式病毒、隐性通道和可恢复密钥的密码等网络信息安全隐患。同时,我军计算机信息网络中所使用的网管设备和软件绝大多数是外来品,在网络上运行时,存在着很大的信息安全隐患。这使得军用计算机信息网络的安全性能大大降低,网络处于被窃听、干扰、监视

和欺诈等多种安全威胁中,信息网络安全处于极脆弱的状态。

### 1.2 计算机信息网络病毒安全威胁严重

当前,计算机信息网络的病毒威胁严重,其可以借助文件、电子邮件、网络等多种方式在网络中进行传播和蔓延,这些病毒基本上都具有自启动功能,主要潜入到军队计算机信息系统的核心与内存,一旦启动将对军用计算机信息网络的软件和硬件设计造成严重的威胁。如果军用计算机信息网络受到感染,它们就会利用被控制的计算机为平台,破坏数据信息,毁损硬件设备,阻塞整个网络的正常信息传输,甚至造成整个军队计算机网络数据传输中断和系统瘫痪。

### 1.3 战场信息在军用计算机信息网络中传输的安全可靠性低

在现代战争中,各种战场信息存储于计算机信息网络或者在计算机信息网络中传输的安全性不高,很容易被敌方截获而造成泄密。特别是在战场信息的传输过程中,由于要经过诸多信息网络的外节点,且难以查证,在任何中介节点均可能被读取或恶意修改,包括数据修改、重发和假冒。如整个计算机信息网络中可能存在某节点在非授权的数据修改,这种修改进入信息网络中的帧并传送修改版本,即使采用某种级别的认证机制,此种攻击也能危及可信节点间的通信;而重发就是重复全部或者部分报文,以产生被授权的效果,当节点拷贝发到其他节点的报文并又重发他们时,若不能监测重发,接收的节点会执行报文内容命令的操作,假如

<sup>1</sup> United States Computer Emergency Readiness Team



报文的内容是关闭网络的命令,则将会使整个计算机信息网络出现严重的后果;假冒是计算机信息网络中一个实体假扮成另个实体收发信息,很多网络适配器都允许网帧的源地址由节点自己来选取或改变,这就使冒充变得较为容易。

## 1.4 计算机信息网络外部、内部攻击威胁严重

军用计算机信息网络中,无防备的电脑很容易受到局域网外部的入侵,修改硬盘数据,植入木马等。在此种情况下,外部入侵者会有选择地破坏网络信息的有效性和完整性,或伪装为合法用户进入网络并占用大量信息网络资源,修改网络数据、窃取、破译机密信息、破坏软件执行,在中间站点拦截和读取绝密信息等。在网络内部,则会有非法用户冒用合法用户的口令以合法身份登录网站后,查看机密信息,修改信息内容及破坏应用系统的运行,有的非法用户还会修改自己的 IP 和 MAC 地址,使其成为合法用户 IP 和 MAC 地址,绕过计算机信息网络管理员的安全设置。

## 2 确保军队计算机信息网络安全的主要技术手段

### 2.1 边界防卫技术

简而言之,边界防卫技术是“御敌于国门之外”的安全防护技术。在计算机信息网络遍布全球的今天,无论是界定军用计算机信息网络还是界定民用计算机信息网络系统的边界是困难的。这主要是因为,计算机信息系统是随着联合作战需求的发展不断扩张或变化的;同时,要保护无处不在的网络基础设施成本是很高的。边界防卫技术通常将安全边界设在需要保护的信息周边,例如存储和处理信息的计算机系统的外围,重点阻止诸如冒名顶替、线路窃听等试图“越界”的行为,相关的技术包括数据加密、数据完整性、数字签名、主体认证、访问控制等。这些技术都与密码技术密切相关。近年来,军用计算机信息网络的公钥技术被普遍接受,该技术能够大大降低密钥管理的风险和主体认证的成本,因此,在未来信息化战争中,基于公钥基础设施(简称为 PKI)的边界防卫技术将在军用计算机信息网络中得到广泛应用。

### 2.2 入侵检测技术

军用计算机信息网络入侵检测技术是发现“敌方”渗透企图和入侵行为的技术。在信息化战争中,军用计算机信息网络系统越来越复杂,以致使用者无法保证系统不存在设计漏洞和管理漏洞。在近年发生的网络攻击事件中,突破边界防卫系统的案例并不多见,黑客们的攻击行动主要是利用各种漏洞长驱直入,使边界防卫设施形同虚设。信息技术的普及和信息基础设施的不完备导致了严峻的安全问题。使用者不得不通过入侵检测技术尽早发现入侵行为,并予以防范。入侵检测技术基于入侵者的攻击行为与合法用户的正常行为有着明显的不同,实现对入侵行为的检测和告警,以及对入侵者的跟踪定位和行为取证。入侵检测系统(简称为 IDS)的确起到了对入侵者的震慑作用。随着在战争中黑客入侵手段的提高,尤其是巧借他人之手实施联合攻击的方法出现,传统单一的、缺乏协作的入侵检测技术已经不能满足需求,分布协同的入侵检测技术成为当今军用计算机信息系统入侵检测技术领域研究热点。

### 2.3 安全反应技术

军用计算机信息安全反应技术是将“敌方”攻击危害降低到最小限度的技术。安全的军用计算机信息网络系统必须具备在被攻陷后迅速恢复的能力。快速响应与恢复的目标是要在开放的互联网环境下构建基于生存性的多样化动态漂移网络,其中分布式动态备份的技术与方法、动态漂移与伪装技术、各种灾难的快速恢复与修复算法等是未来计算机信息网络系统的主要技术发展方向。

### 2.4 数据加密技术

在军用计算机信息网络系统中采用安全性较高的系统和使用数据加密技术,是确保整个信息系统安全与稳定的重要途径。如美国国防部技术标准把操作系统安全等级分为 D1、C1、C2、B1、B2、B3、A 级,安全等级由低到高。目前主要的操作系统等级为 C2 级,在使用 C2 级系统时,应尽量使用 C2 级的安全措施及功能,对操作系统进行安全配置。在极端重要的系统中,应采用 B 级操作系统,对军事信息在网络中的存储和传输可以使用传统的信息加密技术和新兴的信息隐藏技术来提

供安全保证。在传输和保存军事信息的过程中,不但要用加密技术隐藏信息内容,还要用信息隐藏技术来隐藏信息的发送者、接收者甚至信息本身。通过信息隐藏技术、数字水印技术、数据隐藏技术和数据嵌入技术、指纹技术等技术手段可以将秘密资料先隐藏到一般的文件中,然后再通过网络来传递,提高信息保密的可靠性。

## 2.5 防火墙技术

在军用计算机信息网络中,为了确保整个信息系统的安全,在网络中的主机上安装防病毒软件,能对病毒进行定时或实时的病毒扫描及漏洞检测,变被动清毒为主动截杀,既能查杀未知病毒,又可对文件、邮件、内存、网页进行全面实时监控,发现异常情况及时处理。防火墙是硬件和软件的组合,它在内部网和外部网间建立起一个安全网关,过滤数据包,决定是否转发到目的地。它能够控制网络进出的信息流向,提供网络使用状况和流量的审计、隐藏内部 IP 地址及网络结构的稳定,它还可以对军队计算机信息网络系统进行有效的网络安全隔离,通过安全过滤规则严格控制外网用户非法访问,并只打开必须的服务,防范外部来的拒绝服务攻击。同时,防火墙可以进行时间安全规则变化策略,控制内网用户访问外网时间,并通过设置 IP 地址与 MAC 地址绑定,防止目的用户的 IP 地址欺骗。更重要的是,防火墙不但将大量的恶意攻击直接阻挡在网络系统之外,同时也屏蔽来自网络内部的不良行为,让其不能把某些保密的信息散播到外部的公共网络上。

## 2.6 安全路由器和虚拟专用网技术

军用计算机信息系统的安全路由器采用了密码算法和加密、解密专用芯片,通过在路由器主板上增加安全加密模件来实现路由器信息和 IP 包的加密、身份鉴别和数据完整性验证、分布式密钥管理等功能。使用安全路由器可以实现军队各单位内部

参考文献(略)

作者联系方式

通信地址:海南海口市海口警备区

邮政编码:570236

联系电话:0898-66573003

网络与外部网络的互联、隔离、流量控制、网络和信息安全维护,也可以阻塞广播信息和不知名地址的传输,达到保护内部信息化与网络建设安全的目的。目前我国自主独立开发的安全路由器,能为军队计算机网络提供安全可靠的保障。建设军队虚拟专用网(Virtual Private Net),是在军队广域网中将若干个区域网络实体利用隧道技术连接成个虚拟的独立网络,网络中的数据利用加密、解密算法进行加密封装后,通过虚拟的公网隧道在各网络实体间传输,从而防止未授权用户窃取、篡改信息。

## 2.7 网络诱骗技术

在军用信息网络系统中,入侵检测能力是衡量整个防御体系是否完整有效的重要因素。入侵检测的软件和硬件共同组成了入侵检测系统。强大的、完整的入侵检测系统可以弥补军队网络防火墙相对静态防御的不足,可以对内部攻击、外部攻击和误操作进行实时防护,当军队计算机网络和系统受到危害之前进行拦截和响应,为系统及时消除威胁。网络诱骗系统是通过构建一个欺骗环境真实的网络、主机,或用软件模拟的网络和主机,诱骗入侵者对其进行攻击或在检测出对实际系统的攻击行为后,将攻击重定向到该严格控制的环境中,从而保护实际运行的系统;同时收集入侵信息,借以观察入侵者的行为,记录其活动,以便分析入侵者的水平、目的、所用工具、入侵手段等,并对入侵者的破坏行为搜集证据。

军用计算机信息网络中的信息安全从深度上看是一个长期存在的问题,从广度上看是一个包括管理和技术等多个层面的综合体。因此,我军在进行信息化建设的过程中,特别是在构建军用计算机信息网络的过程中,应当充分把握关键点,注重控制权,大胆运用先进技术以综合集成实现信息安全体系的可持续发展,是保障我军信息安全的一个有效途径。

# 全面提升新形势下信息网络安全防护能力

宁作臣 马建民

**摘 要:** 本文就新形势下我军信息网络安全防护问题进行了深入的研究,先后从网络安全面临的形势、安全防护应遵循的基本原则、安全防护应采取的主要方法以及网络安全防护应把握的主要问题进行了详细的阐述,为进一步提高军队信息网络安全防护能力奠定了一定理论基础。

**关键词:** 网络安全; 信息网络; 防护能力

军队信息网络作为我军军事信息系统的重要组成部分,在保障作战指挥、战备值班、训练演习、抢险救灾等方面发挥了巨大作用,已成为不可缺少的指挥手段。新形势下信息网络技术的迅猛发展,军事领域的重大变革,使军队信息网络安全防护工作发生了深刻变化。以抵御技术侦察窃密与破坏、保护涉密信息及系统安全、防止泄密为主要目的的信息网络安全防护工作,已成为各级安全工作的重中之重。为加速推进中国特色军事变革和加紧做好军事斗争准备需要,如何搞好新形势下信息网络安全防护工作,是各级指挥员十分关注的问题,也是当前亟待研究的重要课题。

## 1 新形势下信息网络安全防护工作面临的严峻形势

新形势下,信息网络安全防护关系到信息化建设的全局和未来高技术战争的胜负,主要作战对手的侦察窃密和信息攻击能力处于相对优势,信息网络安全防护工作,面临前所未有的复杂形势和严峻挑战。

### (1) 群体群防意识比较淡薄

信息网络具有整体性强、业务较多、技术链接复杂等特点,网络安全受基础设施建设、管理制度、技术措施、思想观念、组织领导、人员素质等诸多因素影响,因此必须树立“全网、全程、全时、全员”的整体防护意识。切实使广大官兵认识到信息网络安全面临的严峻形势,增强忧患意识,将信息网络安全问题视为保持部队稳定和夺取未来对敌斗争胜利的重要因素,把思想统一到“保安全就是保打赢”上来,树立“网络安全,人人有责”的观念,加强信息网络的内部规范,努力营造一个

群策群力、群治群防的良好环境。

### (2) 安全防护手段相对滞后

随着信息网络的发展与应用水平的广泛应用,信息网络建设有了较快发展,应用效益明显提高,极大地促进了部队信息化和指挥手段的建设。但是,我们必须看到已建成的信息网络,一些核心技术还依赖于引进,尤其是操作系统及应用软件,大部分被国外所垄断,存在被预先设置“后门”与“陷阱”的可能性。大量采用网络互联技术,协议的开放性易造成网络边界难确定、网络行为难监控,面临遭敌渗透、欺骗、窃密和攻击的危险。目前采用的所有安全手段主要是以共享信息资源为中心在外围对非法用户和越权访问进行封堵,以达到保护的目的,而对共享源的访问者源端不加控制,加之操作系统与各类应用系统的漏洞层出不穷,无法从根本上解决安全问题。

### (3) 规章制度建设有待加强

信息网络安全不仅涉及到技术问题,而且涉及到法规制度和行政管理问题。现行的条令条例对信息网络安全防护内容的规范不够具体,缺乏针对性、操作性的依据。网络管理使用人员防范信息攻击的警觉性不高,重用轻管、重用轻防、重用轻密的现象比较普遍,容易给敌侦听窃密、袭扰破坏、恶意攻击造成可乘之机。从信息网络专业队伍建设的情况看,安全监管力量明显不足,专业人员的防范素质不够强,对引进设备的安全性能综合分析水平不高,出现突发情况缺少及时有效的应急措施。

### (4) 操作规程执行不够规范

在信息网络安全防护过程中,仍存在着措施落实不到位,操作规程不够规范的问题。主要表现在:操作中随意性比较大,文件的共享不设密码或

加密口令字长不符合规定八位；在无加密设施的情况下，传输涉密文件或涉密文件、资料上网等；访问控制不够严谨，个别单位甚至将部队作战、训练的一些资料上网，但对合法的用户没有进行严格的访问控制，使其可以进行越权访问，容易给别有用心的人提供可乘之机。

## 2 新形势下信息网络安全防护必须遵循的基本原则

信息网络安全防护必须以建设信息化军队、打赢信息化战争为目标，加强统筹规划，深化依法管理，依靠科技进步，努力建设体制科学、技术先进、法规健全、保障有力的信息网络安全防护体系，以有效提高计算机安全防护能力。

### （1）统一领导的原则

信息网络安全防护工作涉及方方面面，没有集中统一领导，既形不成合力，更难见效，还容易造成人力、物力、财力上的极大浪费。必须按照“谁主管谁负责”的原则，进一步健全保密管理体制，明确部门职责，完善工作制度，加大统一领导，逐步形成责权分明、协同高效的安全防护机制。加强协调，密切配合，分级负责，科学制定安全防护措施，强化横向联系和纵向管理，确保信息网络安全防护工作顺利健康地向前发展。

### （2）积极防范的原则

根据新的形势任务需要，进一步完善计算机信息网络安全管理规定，规范涉密电子文本的使用管理办法，尽快形成科学严谨、系统配套、便于操作的信息安全保密法规体系。加快完善信息网络安全标准化进程，抓紧制定符合战区实际的信息网络安全管理和技术标准以及配套实施办法，逐步建立与军队标准相衔接、适应战区军事斗争需要的信息网络安全防护标准体系。对可能发生的情况，主动采取防范措施，对敌可能的攻击行动，及早发现征候，果断应对处置。

### （3）技管并举的原则

坚持技术防护与行政管理相结合，注重运用先进技术提高管理水平，通过科学管理增强技术效能，综合治理，系统防护。把发展具有自主知识产权的信息安全保密技术与产品，作为科研开发的重要任务。有效聚合军内外科研优势，充分依托国家和社会资源，加强关键技术攻关，加快构建自主可

控的信息网络安全防护平台。加大信息网络安全防护检测技术的研究力度，大力提高信息网络安全防护技术的整体水平。健全完善信息网络安全防护测评认证机制，做好信息网络安全防护技术与产品的安全把关和应用推广工作，保证先进技术和产品的优先应用。严禁使用未经军队主管部门测评认证的信息安全保密技术与产品。

### （4）同步发展的原则

坚持信息安全保密建设与信息化建设统筹规划，同步实施，做到信息网络安全防护建设必须与项目建设同步设计、同步实施、同步验收。在建和已建涉密信息网络，必须按照有关规定划定安全防护等级，完善安全保密设施，并采取防范擅自接入国际互联网的技术措施。加强对计算机信息系统的安全保密监控，建立定期检查评估制度。加快应急机制建设，不断提升计算机信息系统的动态防护和应急处置能力。加大对军事设施及其环境的保护力度，重要涉密场所、核心要害部位，必须采取防窃密、泄密措施。

## 3 新形势下信息网络安全防护主要采取的方法

消除信息网络安全隐患，增强系统的稳固性，应从以下几个方面下功夫。

### （1）要周密设计，阻漏防渗

在网络建设的过程中，要严格实行指控网络与民用互联网的物理隔断，并建立相对独立的应急作战指控系统。为防止涉密信息通过电磁波辐射或物理接近方式被非法接收，信息系统设备要建在屏蔽室（柜）内；涉密信息系统的内网、外网的布线必须要有一定的间距，涉密网布线要使用屏蔽线或者是光纤。同时，要注重网络系统自身的脆弱性，严格网络设备和软件系统的安全检测认证，随时更新身份认证和网络参数。操作系统是计算机资源的直接管理者，是连接计算机硬件与上层软件及用户的桥梁，所以操作系统本身的安全性尤为重要。运用身份鉴别机制来保证系统安全，在口令基础上运用令牌组合方式来对使用者身份进行鉴别；适当时期运用访问控制机制，对用户访问采取指纹、视网膜和身份卡控制，实现系统在强制访问控制下进行身份认证，从而界定用户是否可以访问某个文件或进行某项操作。

### (2) 要定期登录, 重点防范

采取定期登录的办法, 对节点机和服务器进行经常性登录核查, 重点检查服务器运行日志有无非法登录和超常进程, 对非法占用控制终端的超级用户, 一旦发现, 应立即关断路由器等网络入口, 启动备用节点机和服务器。同时, 随时检查用户注册表和进行系统文件重新登录操作, 定时更换口令和密码, 改变重要网址, 调整寻址方式, 并根据主机服务器的登录记录对上网终端进行排查, 特别要检查服务器中有无“特洛伊木马”、“蠕虫”等隐藏程序和文件, 斩断“黑客”的上网黑手, 保证设备安全。

### (3) 要以管助防, 加强防范

由于计算机病毒可以通过计算机存储介质(磁盘、光盘)传播, 因此, 加强网络使用人员和存储介质的管理, 是防止病毒内部感染的一个重要环节。因此, 首先要提高网络使用人员, 特别是网管人员的政治觉悟, 增强他们的使命感和工作责任心, 要认真贯彻执行条令、条例, 落实各项保密制度, 特别对存储介质的进与出要严格把关, 消除内部感染病毒的各种隐患, 使敌策反找不到内部缺口, 间谍渗透无从下手。对主干系统进行全时、全程信息监控, 可及时启用新的保密芯片, 利用防火墙、防病毒软件和保密终端来控制用户可访问的涉密信息资源范围以及可执行的操作。对网络信息中心(MC)、节点、重要的信道和终端进行电磁屏蔽。对末端设备和网线隐真示假, 使病毒难寻入网途径。

### (4) 要攻防兼备, 灵活抗毁

在加强指挥信息系统被动防护的同时, 通过软、硬手段结合, 对敌实施主动信息攻击, 削弱和破坏其信息进攻能力, 减轻我信息系统防护压力, 达到以攻助防的目的。综合运用各种手段, 适时运用电子干扰、网络攻击等手段, 对敌预警探测、电子干扰、反辐射武器等信息作战系统实施干扰压制和破坏, 削弱其信息进攻能力。同时, 要发挥我既设网络密集的优势, 利用不同程式、不同频段的无线电设备, 大量采用混合组网、复式组网、立体组网、多径组网或建立隐蔽网、备用网等方式, 达到此断彼通, 多网保通的目的。要因情制宜, 灵活处置, 敢于打破常规定势, 为作战指挥提供安全的信息处置中枢。

## 4 新形势下信息网络安全防护需要把握的几个问题

新形势下信息网络安全防护, 必须坚持人防、技防和制度的有机结合, 才能保证信息网络系统的物理实体免遭破坏, 保证系统安全稳定可靠地运行。

### (1) 建立健全制度, 坚持科学正规管理

加强信息网络安全防护工作, 必须坚持技术防护与管理并重的原则, 特别在技术比较落后的情况下尤其要加强管理。没有严格的管理, 防护技术再先进也难以奏效。因此, 必须把强化管理放在突出的位置上, 下大力气抓好建章立制的工作, 要针对网络建设及安全保密方面存在的问题和薄弱环节, 围绕管住人、设备和涉密信息, 建立完善各项规章制度, 狠抓安全工作落实。首先要严把用户上网关。如建立入网审批制度, 规范上网程序, 建立用户档案, 定期抽查上网记录。其次要狠抓网络运行关。通过集中网管、实时监控等手段, 提高网络安全管理水平。第三要建立网络使用、信息发布、人员控制等相关法规, 坚持依法治网。第四要建立网络安全定期评估制度。网络安全是一个动态过程, 没有一劳永逸的解决方案, 必须定期调整安全策略, 不断加入新技术。通过各种制度来规范网络的使用和管理, 形成标准明确、要求具体、操作性强的法规体系。同时, 加强检查督促, 坚持赏罚分明, 使信息网络安全防护工作逐步走上依法管理的轨道。

### (2) 完善管理机制, 狠抓各项职责落实

信息网络安全防护工作覆盖各个领域, 涉及多个部门, 技术含量高, 管理难度大, 必须实行统一领导, 建立完善相关机制, 各个部门要分工负责, 齐抓共管。《指挥自动化条例》中明确规定:“指挥自动化系统的电子防御、网络安全防护、安全保密、系统防卫等工作分别由电子对抗、指挥自动化、机要、作战等主管部门牵头, 会同有关部门, 加强分工与合作, 严密组织。”要针对信息网络安全工作中存在的问题, 综合运用行政和技术手段, 实施全过程的管理和动态监控, 确保各项规章制度的落实。在抓信息网络安全防护工作中, 必须按照归口管理的原则, 各司其职, 各负其责, 充分发挥自身的职能作用, 切实加强信息网络安全防护工作。

### （3）坚持创新发展，加强核心技术研发

信息网络安全防护，必须按照“先进、科学、可靠、适用”的原则，围绕“非法用户进不来，秘密信息取不走，网络基地摧不垮”的目标，加大科技投入。通过采用防火墙、漏洞扫描、预警检测、实时监控、防病毒、信息加密等先进技术措施，保护核心机密信息不被窃、不失密，做到“处处加密，层层设防”，建立起既有宏观监控功能，又有各环节技术保护措施立体性技术防护体系。同时，要积极贯彻“立足现实、着眼发展、整体规划、突出重点、自主开发”的方针，把自主开发与引进技术、军队开发与地方开发、基础技术研究与防护技术研究相结合，找准“切入点”，选定“突破口”，重点抓好以信息网络安全为基础、密码技术为支撑的“杀手锏”和急需产品的研制，努力提高信息网络防护能力，尽早摆脱技术受制于人的被

动局面，形成具有一定安全防护能力的自主体系。

### （4）抓好人才培养，提高应急响应能力

信息网络是高科技发展的产物，网络攻防是人才、智能和技术的较量，做好网络安全防护工作，关键在人的素质，尤其是职业道德和科技素质。如果涉网人员不具备相应的职业道德素质和科技素质，即使设施再完备，也不能发挥其应有的作用。**一方面**要采取有力措施，搞好信息网络安全防护知识的宣传教育，营造良好的网络安全防护氛围。教育广大网络管理人员和操作人员加强职业道德修养，自觉按章办事，责无旁贷地做好信息网络安全防护工作。**另一方面**要搞好技术培训，采取多种形式组织有关人员学习信息网络安全防护常识和规定，掌握必要的应用技能，努力实现“人-机”的最佳结合，充分发挥技术设备的安全防护作用。

## 参考文献

- [1] 杨义先，钮心忻，任金强主编.《网络信息安全与保密(修订版)》.北京：北京邮电大学出版社，2001
- [2] 黄月江等编著.《信息安全与保密》.北京：国防工业出版社，1999
- [3] 戴守坤等编著.《信息系统安全》.北京：金城出版社，2001

## 作者联系方式

通信地址：北京市石景山区八大处甲1号104信箱

邮政编码：100041

联系电话：010-66399874

# 一种军用RBAC扩展模型及其实现研究

葛方斌 王建新 杨林

**摘 要:** 根据军事信息系统的访问控制需求, 提出了一种 RBAC 扩展模型。扩展模型通过角色类型划分与权限交叉控制机制合理约束了角色权限; 通过安全标记机制实现了细粒度的灵活的角色权限指派; 通过角色授权约束机制实现了重要角色的监督。另外, 提出了扩展模型的一种实现架构, 该架构符合 RBAC 参考管理规范, 具有良好的扩展性, 可满足多种应用环境的需求。

**关键词:** RBAC; 管理域; 安全标记; 授权约束

ISO 在深入研究 OSI 环境安全性的基础上提出了 OSI 安全体系<sup>[1]</sup>, 该体系定义了五种标准的安全服务, 访问控制安全服务是其中之一。访问控制是对资源使用条件的规定, 提供了对越权使用资源的防御措施。一个良好的访问控制机制除了能阻止越权行为外还应具有一定的灵活性, 合理的访问请求必须尽可能得到满足。

军事指挥信息系统是一个有着高安全要求的专用系统, 访问控制当然是系统中不可或缺的安全机制。军事指挥信息系统的访问控制采取的是强制方式, 使用模型以 BLP<sup>[2]</sup>为代表。但该模型存在一些明显的局限性, 主要有两个方面, 一是访问控制的灵活性较差, 容易出现合理访问遭拒绝的情况, 影响了系统的可用性; 二是以安全标记支配关系为基础的权限设置难以准确反映主体职责的权限要求, 访问控制不能很好地贯彻最小权限原则, 对系统的安全性造成了不利影响。基于角色的访问控制 (RBAC) 模型为解决这些问题提供了一个很好的选择, 该模型的基本思想是, 在用户和权限之间引入角色中介, 用户通过分配适当的角色获得访问授权。实现了用户和权限的逻辑分离, 既简化了权限管理, 同时也方便了最小权限原则的实施。与传统的自主访问控制 (DAC) 和强制访问控制 (MAC) 相比, RBAC 更贴近系统实际环境, 具有更好的灵活性和扩展性。

自从 RBAC96 模型<sup>[3]</sup>被提出以后, 关于 RBAC 的研究大量涌现, 但这些研究大多局限于概念模型的特征性质等方面<sup>[4,5,6]</sup>, 真正面向具体领域的应用模型研究并不多。以下从军事指挥信息系统访问控制需求的实际出发, 借鉴有关概念模型的成果, 在此基础上建立一个可用于军事指挥信息系统的基于

角色的访问控制模型, 并给出模型的实现架构。

## 1 军事指挥信息系统的访问控制需求

军事指挥信息系统的访问控制策略应具备用于实战环境的足够的灵活性与保密性, 能依据具体的任务、规定的职权职责对所需的信息进行所需的访问。系统由众多的独立管理域组成, 这些管理域承担的任务职责相似, 但各自的等级层次有所差别, 这些差别要求不同域中的同类型主体在访问权限上应有所区分, 层次较高域的主体一般拥有更大的权限。系统中所有参与用户都有相对固定的职责, 用户的权限应和其职责相匹配, 这需要给每个用户赋予一定的角色身份。另外, 当系统中出现重组、伤亡等人员变更时, 要保证系统能根据需要及时做出调整, 并要求调整不会影响系统的可用性安全性。

从上面分析可以看出, 对于军事指挥信息系统而言, 基于角色的访问控制是其合理的选择。它在权限的合理配置、访问控制的灵活性安全性等方面都能满足军事指挥信息系统的需求。当然, 由于基本 RBAC 模型只涉及用户、角色、权限、约束等一般性概念, RBAC 用于军事指挥信息系统需要进行适当的扩展。

军事指挥系统一般由众多等级不一的指挥机构组成。所有这些指挥机构按照所在部别之间的隶属关系形成树状的层次结构, 树的每一个节点都是一个独立的管理域。管理域内部和管理域之间的信息交换都满足一定安全策略的约束。

军事指挥信息系统中由于有众多的岗位和管理域, 因此系统中角色也比较多。但根据所承担任务的不同角色可简单分为两类: 管理角色和应用角

色。管理角色包括系统管理员、系统操作员、安全管理员和安全操作员，主要担负系统功能的维护以及安全策略的制定与实施。由于这些角色对系统正常运行和安全的至关重要性，应禁止其他角色继承这些角色的权限，并且管理员和操作员应当是严格职责分离的。系统管理员负责制定系统功能配置的修改维护计划，系统操作员负责计划的具体实施。安全管理员负责安全策略的制定修改，安全操作员负责安全策略配置修改的具体实施。应用角色包括军事指挥员、指挥协理员、参谋人员、信息采集员和信息处理员。指挥员是本级管理域各部门工作的总负责，负责授权本域人员的工作及军事指令信息的制定发布等，能继承指挥协理员、参谋人员等其他角色的全部或部分权限。每个域的指挥员角色只能由一个用户担任，考虑到重组伤亡等突然的人员变化情况，指挥员角色应设有临时授权用户，以备指挥员用户缺位时指挥功能的正常行使。指挥协理员在指挥员的授权下承担指挥员的部分职责。参谋人员辅助指挥员进行指挥决策。信息采集员负责各种作战相关信息的收集。信息处理员负责对各种信息的归类整理并进行相关分析，为各种决策提供准确直观细致的参考依据。

军事指挥信息系统涉及的信息可分为三类：基础情报信息、辅助决策信息和指令信息。基础情报信息包括敌我双方军力信息和战场环境信息。军力信息涉及部队部别、人员构成、装备情况、作战能力、作战部署、后勤保障情况等。战场环境信息包括地形、物况、气象大气、海洋水文、声波电磁波传播环境等信息。辅助决策信息是基础情报信息归类分析的结果，具有直观、详实、易理解的特点，是各种决策的主要依据。信息除了类型的不同外还有密级高低之分。例如，不同等级指挥机构发布的指令信息其机密等级也有所不同，机构等级越高，发布的指令信息等级也越高。对这些信息的访问应严格遵循“需要知道”原则，与访问用户职责无关的信息一律禁止用户的访问。

## 2 扩展的RBAC模型

### 2.1 模型要素

设  $D$ 、 $U$ 、 $R$ 、 $S$ 、 $OP$ 、 $OB$  分别是管理域、用户、角色、会话、操作、对象集。

$R$  由管理类角色  $R_{ad}$  和应用类角色  $R_{ap}$  组成，即  $R = R_{ad} \cup R_{ap}$ 。每个角色  $r \in R$  都是一个二元组  $(name, d)$ ， $name$  是角色名， $d \in D$  表示  $r$  所在的域。

$OP$  包括读  $\underline{r}$ ，写  $\underline{a}$ ，创建  $\underline{c}$ ，删除  $\underline{d}$

$OB$  分两类，系统对象  $OB_s$  和应用文件对象  $OB_a$

权限集合  $P$ ： $P \subseteq OP \times OB$

域函数  $dom : U \cup R \cup OB \rightarrow D$ ，指定每个用户、角色、对象的所在域

$TYPE = \{type_1, type_2, \dots, type_m\}$ ：应用文件对象的类型集合

$CLASS$ ：等级集合。 $CLASS = CLASS_{\underline{r}} \cup CLASS_{\underline{a}} \cup CLASS_{\underline{c}} \cup CLASS_{\underline{d}}$ ，其中， $CLASS_{\underline{r}}$ 、 $CLASS_{\underline{a}}$ 、 $CLASS_{\underline{c}}$ 、 $CLASS_{\underline{d}}$  分别代表读、写、创建、删除等级集合，每类等级集合的元素之间存在全序关系，所有等级集合的最小元统一用  $\varepsilon$  表示， $\varepsilon$  只分配给角色，而不分配给对象，用于对角色的某一种操作权限的完全禁止。

对象安全标记集合：

$LABEL_{OB} \subseteq LABEL = \{(type, c^{\underline{r}}, c^{\underline{a}}, c^{\underline{c}}, c^{\underline{d}}) | type \in TYPE, c^{\underline{r}} \in CLASS_{\underline{r}}, c^{\underline{a}} \in CLASS_{\underline{a}}, c^{\underline{c}} \in CLASS_{\underline{c}}, c^{\underline{d}} \in CLASS_{\underline{d}}\}$

对象安全标记指派函数： $f_{OB_a} : OB_a \rightarrow LABEL_{OB}$ ，给每个应用对象指定一个安全标记。

安全标记支配关系：

设  $label_1, label_2 \in LABEL$ ，

$label_i = (type_i, c_i^{\underline{r}}, c_i^{\underline{a}}, c_i^{\underline{c}}, c_i^{\underline{d}})$  ( $i=1,2$ )，则

$label_1$  读支配  $label_2$ ，当且仅当  $type_1 = type_2 \wedge c_1^{\underline{r}} \geq c_2^{\underline{r}}$ ，记为  $label_1 \triangleright^{\underline{r}} label_2$

$label_1$  写支配  $label_2$ ，当且仅当  $type_1 = type_2 \wedge c_1^{\underline{a}} \geq c_2^{\underline{a}}$ ，记为  $label_1 \triangleright^{\underline{a}} label_2$

$label_1$  创建支配  $label_2$ ，当且仅当  $type_1 = type_2 \wedge c_1^{\underline{c}} \geq c_2^{\underline{c}}$ ，记为  $label_1 \triangleright^{\underline{c}} label_2$

$label_1$  删除支配  $label_2$ ，当且仅当  $type_1 = type_2 \wedge c_1^{\underline{d}} \geq c_2^{\underline{d}}$ ，记为  $label_1 \triangleright^{\underline{d}} label_2$

$label_1$  完全支配  $label_2$ ，当且仅当

$label_1 \triangleright^{\underline{r}} label_2 \wedge label_1 \triangleright^{\underline{a}} label_2 \wedge label_1 \triangleright^{\underline{c}} label_2 \wedge label_1 \triangleright^{\underline{d}} label_2$



记为  $label_1 \triangleright label_2$

安全标记是对象安全属性的反映, 对象的读、写、创建、删除支配等级越高, 能对该对象进行相应操作的角色主体一般越少。

角色安全标记集合:  $LABEL_R \subseteq 2^{LABEL}$

角色安全标记指派函数  $f_R: R \rightarrow LABEL_R$

用户角色指派  $UA: UA \subseteq U \times R$ , 用户与角色间的多对多映射。

角色权限指派  $PA: PA \subseteq R \times P$ , 角色与权限间的多对多映射。角色权限指派分为显式指派和隐式指派两种, 显式指派是将权限和角色直接关联, 管理角色的权限指派属于显式指派。隐式指派是通过角色和对象的标记支配关系来关联角色和权限, 对应用角色的权限指派属于隐式指派。

角色权限显式指派函数  $P\_assign: R_{ad} \rightarrow 2^P$ , 指定每个管理角色可获得的权限集合。

对象创建函数  $create: OB \rightarrow U$ , 将对象映射到其创建用户。

角色关系:

角色互斥关系  $ER \subseteq R \times R$ : 为了防止用户的欺骗行为以及减少用户操作出错的可能性, 某些角色对要求不能分配给同一个用户, 这样的角色对称称为互斥角色。例如, 安全管理员角色和安全操作员角色。角色互斥关系具有反自反性和对称性, 但一般不具有传递性。

角色授权约束关系  $PR \subseteq R \times R$ : 从安全的需求出发, 某些角色的行为需要其他角色的监督, 被监督角色的操作要求获得另外某个角色的授权。例如, 指挥协理员需要军事指挥员的授权才能行使其权限。 $(r_1, r_2) \in PR$  表示角色  $r_1$  的操作需要经过角色  $r_2$  的授权。

## 2.2 模型规则

**规则 1** 用户、角色、对象组织规则

每个用户、角色、对象都有唯一所在域

- a)  $\forall u \in U (\exists d \in D (u \in d) \wedge (u \in d_1 \wedge u \in d_2 \rightarrow d_1 = d_2))$
- b)  $\forall r \in R (\exists d \in D (r \in d) \wedge (r \in d_1 \wedge r \in d_2 \rightarrow d_1 = d_2))$
- c)  $\forall o \in OB (\exists d \in D (o \in d) \wedge (o \in d_1 \wedge o \in d_2 \rightarrow d_1 = d_2))$

**规则 2** 角色权限分类约束规则

管理角色只能拥有对本域系统对象的操作权限, 应用角色只能拥有对应用对象的操作权限

a)  $\forall r \in R_{ad} \wedge \forall (x, o) \in P\_assign(r) \rightarrow$

$o \in OB_{ad} \wedge dom(r) = dom(o)$

b)  $\forall r \in R_{ap} \wedge \forall (x, o) \in P\_assign(r) \rightarrow o \in OB_{ap}$

其中,  $x \in \{r, a, c, d\}$

**规则 3** 对象创建规则

用户创建对象的安全标记完全支配于用户拥有的某个角色安全标记中的某个元素。用户的创建对象是用户可读可写可删除的。

$create(o) = u \rightarrow \exists r \in R \exists label \in f_R(r) ((u, r) \in AU \wedge label \triangleright f_{OB}(o))$

**规则 4** 角色权限指派约束规则。

应用角色  $r$  拥有对对象  $o$  的  $x$  权限, 则  $r$  的安全标记中必有某标记 “ $x$ ” 支配  $o$  的安全标记。应用角色的访问可不受域的限制, 访问授权依据的是角色标记和对象标记的支配关系。

$r \in R_{ap} \wedge (r, (x, o)) \in PA \rightarrow \exists label \in$

$f_R(r) (label \triangleright^x f_{OB}(o))$

**规则 5** 用户角色指派约束规则

具有互斥关系的两个角色不能指派给同一个用户。

a)  $(u, r_1) \in UA \wedge (u, r_2) \in UA \rightarrow \neg (r_1, r_2) \in ER$

一个角色所能分配的用户数必须不超过其约束基数

b)  $\forall r \in R (|U_R(r)| \leq num_r)$

其中,  $U_R(r) = \{u \in U | (u, r) \in UA\}$ ,  $num_r$  是角色  $r$  的约束基数。

**规则 6** 角色激活约束规则

$(r_1, r_2) \in PR \rightarrow pred(r_1, r_2)$

其中,  $pred$  是一个二元谓词,  $pred(r_1, r_2)$  表示角色  $r_1$  的激活需要  $r_2$  的授权。

## 2.3 用户授权过程

1) 用户提交身份信息, 身份认证机构对用户合法性进行认证, 通过认证的用户允许登录系统, 否则, 拒绝登录。

2) 登录用户在一定的会话创建约束下创建一个会话。

3) 会话创建用户请求角色激活, 当请求激活

的角色在用户角色指派中，且符合激活约束条件时，获准激活，否则，拒绝激活请求。

4) 用户使用其激活角色身份提交访问请求，系统访问控制模块检查相关条件，对请求做出决策。对请求的授权分三种情况。

- 请求的对象是系统对象。系统访问控制功能模块检查用户所在域及角色身份，如果用户与请求对象所在域相同，且请求权限在用户角色的权限指派中，则对请求授权，否则，拒绝访问。
- 请求的对象是本域的应用文件对象。如果用户角色是应用类角色，且角色的某个安全标记元在请求操作上支配对象的安全标记，则对请求授权，否则，拒绝访问。
- 请求的对象是外域的应用文件对象。首先由外域认证机构验证用户身份的合法性，其他授权条件的验证与前一种情况相同。

2.4 模型主要特点

上述模型从管理域划分、角色对象分类、模型约束、角色权限指派管理等方面对基本 RBAC 模型进行了扩展，很好地适应了军事指挥信息系统的访问控制需求。模型的主要特点包括如下几个方面。

- 1) 将访问控制从单管理域扩展到多管理域，能满足分层或分布式环境的访问控制需求。
- 2) 将角色分为管理类和应用类，严格限制两类角色的权限交叉，使特权角色的权限得到适当控制，提高了系统的安全性。
- 3) 在角色权限管理中加入了安全标记控制机制。安全标记等级根据对象类型的不同区别设置，实现了细粒度的角色权限指派，方便了最小权限原则的实施，简化了权限管理，提高了角色权限指派的灵活性。
- 4) 在模型约束中加入了角色授权约束。模型中角色的权限各有不同，某些角色的权限具有较高的安全风险性，角色授权约束实现了对这些角色的安全监督，进一步提高了系统的安全性。

3 模型实现架构

为了统一各种 RBAC 实现，NIST 在参考标准中提出了 RBAC 的管理规范，以下给出一个符合

该参考管理规范的 RBAC 系统的实现架构。如图 1 所示。该架构不仅可以用于上述扩展的 RBAC 模型，更是一个通用的架构，可满足多种环境的需求。

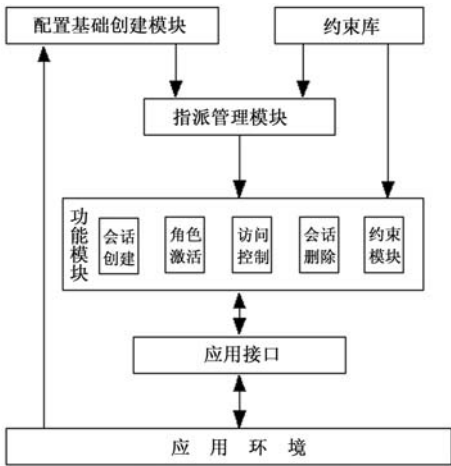


图 1 RBAC 模型实现架构

实现架构由六个部分组成。配置基础创建模块、约束库、指派管理模块、功能模块、应用接口和应用环境。

(1) 配置基础创建模块

配置基础创建模块通过参考标准的管理函数创建并维护系统域、用户、角色、操作、对象、类型以及安全标记等的名称和标识，当应用环境中的这些创建对象情况发生变化时，能通过添加删除等操作及时调整创建的对象。为了便于系统功能模块的处理，创建对象的描述语言使用 XML。对约束策略和指派的描述使用同样的语言。

(2) 约束库

约束库是模块化结构体，包含了访问控制的各个环节中常见约束（例如，职责分离约束、基数约束、条件角色约束、时间约束、角色激活约束等）策略的描述。在实际使用环境中，可根据需要选择合适的约束策略。同时，也可在约束库中添加新约束，以满足具体的应用需求。

(3) 指派管理模块

对系统的用户角色以及角色权限进行指派。在上述扩展的模型中，用户角色指派是显式指派，角色权限指派包含显式和隐式两种，对管理角色的权限指派是显式的，权限直接赋予角色，对应用角色的权限指派是隐式的，隐式指派是通过赋予角色和权限以安全标记，通过安全标记支配关系间接赋予角色权限。无论是哪种指派，都应考虑系统要求的

指派约束。指派同样是可以根据需要进行调整的,当使用环境变化时,指派的形式、约束等应能调整以适应需求。

#### (4) 核心功能模块

核心功能模块负责实现会话创建、角色激活、访问控制、会话删除以及相关约束功能。为了屏蔽应用环境的复杂性,功能模块的实现应用环境中的基本元素进行了适当的抽象,每个模块通过应用接口向应用环境提供服务支持。

核心功能模块提供了下列功能接口

`I_session_creation`

`I_role_activation`

`I_access_control`

`I_session_deleting`

`I_constraints`

约束功能由应用环境需要的若干约束模块来实现。各功能模块之间存在一定的逻辑关联性,需要有秩序的配合才能起作用。例如,如果系统包含激活约束模块,则角色激活需要激活约束模块的参与才能行使其功能。

#### (5) 应用接口

应用接口为应用环境提供了一部分管理类函数,这些管理函数包含在下列功能接口中。

`I_user`

`I_role`

`I_operation`

`I_object`

这些功能接口对应用环境中的 RBAC 元素进行了抽象,每个接口提取 RBAC 基本元素并生成相应的标识。

#### (6) 应用环境

应用环境是系统实际的服务环境。系统的配置信息以及约束策略库中约束策略的选择都依赖于应用环境。

上述实现架构具有良好的扩展性。当应用环境变化时,系统需要在约束方面进行调整,在上述架构中只需添加或替换相关的约束功能模块就可实现。

## 4 结束语

RBAC 是适应性极强的访问控制模型,其一般框架可用于众多领域,但各领域在管理方式、约束控制等方面的不同对模型提出了不同的要求。针对军事信息系统特殊的访问控制需求,对基本 RBAC 模型进行了扩展,在模型中增加了管理域概念,根据角色属性不同对角色进行了分类,通过权限交叉控制对特权角色权限进行适当限制,将安全标记引入角色权限指派中,增加了对角色的授权约束。扩展的模型不仅具有高安全特性,同时也具有很好的灵活性,权限的管理也是方便的。模型的实现架构符合 RBAC 参考管理规范,具有良好的通用性和扩展性。

## 参考文献

- [1] 张世永 网络安全原理与应用[M] 北京:科学出版社,2003
- [2] D E Bell, L J LaPadula Secure computer system: Unified eposition and MUL TICS interpretation. The MITRE Corporation, Technical Report: MTR - 2997 Revision1, 1976
- [3] Sandhu R, Coyne E, Feinstein H et al. Role-based access control model [J]. IEEE comptrter, 1996: 29(2) 38-47
- [4] David F Ferraiolo Ravi S Sandhu Serban Gavrila et al proposed NIST standard for role-based access control [J] ACM transactions on information and system security 2001, 3(4): 182-186
- [5] Al kahtani M. Sandhu R. Induced role hierarchies with attribute-based RBAC [C] proceedings of the 8<sup>th</sup> ACM symposium on access control models and technologies. Villa Gallia. 2003: 142-148
- [6] keiji Izaki , Katsuya Tanaka, Makoto Tskizawa, Information flow control in role-based model for distributed objects. In: Proc of the 8<sup>th</sup> Int'l Conf on Parallel and Distributed Systems. Los Alamitos, CA: IEEE Computer Society Press, 2001, 363—370

## 作者联系方式

通信地址:北京丰台区大成路13号A01

邮政编码:100039

联系电话:13426281691

# 内网安全不容忽视

石雄 赵雯

**摘 要：**在网络安全建设上，“重防外，轻防内”无疑会给网络留下安全隐患。本文分析了内部网络常见的安全隐患，从技术保障和管理规章的不同角度，就如何建立一个可信并可控的内部网络阐述了自己的观点。

**关键词：**内部网络；信息；网络安全

随着信息化建设的深入，各单位、各部门已经广泛使用计算机网络开展日常工作和业务，但是越来越庞大的网络及其不断更新的相关技术也带来了不断增长的安全威胁，计算机网络各方面的安全已经成为一个急待解决的问题，信息化的发展必然要求信息安全技术同步发展作为保障。防病毒、入侵检测、网络隔离、漏洞扫描、防火墙等是人们常用的防止外来网络侵害的传统信息保护手段。然而更大的安全威胁来源于网络内部，内网安全已日渐成为信息安全领域的一个重要组成部分。

## 1 正确认识内部网络信息安全形势

现在一提到信息安全，人们首先想到的就是病毒、黑客入侵，在媒体的宣传下，病毒、黑客已经成为危害信息安全的罪魁祸首。然而，对计算机网络造成重大破坏的往往不是病毒、黑客，而是组织内部人员有意或无意对信息的窥探或窃取。从技术上来讲，内部人员更易获取信息，因为内部人员可以很容易地辨识信息存储地，另外也不需要他们拥有精深的 IT 知识，只要会操作计算机，就可以轻易获取自己想要的资料。相对而言，黑客从外部窃取资料就比较困难，首先他们要突破防火墙等重重关卡，然后还要辨别哪些是他们想要的信息，这就对黑客提出了比较高的技术要求。防火墙、防病毒、信息加密、入侵检测、网络隔离等已经基本解决了抵御外来入侵的困扰，内网安全引起的信息泄密问题成为当前信息安全的新的焦点。

首先，内部网络安全措施简单，防范脆弱。只要内部人员使用简单的网络窃取工具（黑客工具）就可以很容易非法使用、窃取保密数据或对数据进行破坏。同时，内部网络数据管理本身也很薄弱，

核心机密数据通常仅采用简单的口令来保护，而对于正在开发过程中的各种技术资料就更没有任何防护手段，至少对项目组成人员来说，全部的数据和资料都是共享的，几乎没有采取任何措施来防止数据破坏和资料失窃。因此，在内部网络中非法篡改数据和越权获取资料就变得非常容易，而且还不留下记录和证据，给事后追查带来很大的麻烦。另外，内部人员随意安装、使用可移动的存储设备以及随意更改 IP 地址等行为也有发生。除此之外，信息通过非法外联泄露也成为内部网络安全需要解决的一个重要问题。由于网络的复杂性和隐蔽性，加之内部人员最容易接触敏感信息，对单位的结构、制度、运作等情况非常熟悉，导致他们行动时针对性强，不容易被察觉，事后难以发现，使得组织内部的机密信息更加容易透过网络（如私自拨号、一机两用等情况）被有意无意的泄露出去，其造成的危害和损失有时甚至大大高于直接的数据破坏。

目前来看，内部泄密主要通过如下途径来实现：

- 将资料通过软盘、U 盘或移动硬盘从电脑中拷出带走。
- 由互联网将资料通过电子邮件发送到自己的邮箱。
- 将文件打印后带出。
- 将办公用便携式电脑直接带回家中。
- 电脑易手后，硬盘上的资料没有处理，导致泄密。
- 随意将文件设成共享，导致非相关人员获取资料。
- 移动存储设备共用，导致非相关人员获取资料。

- 将自己的电脑登入局域网，窃取资料。
- 乘同事不在，开启同事电脑，浏览、复制同事电脑中的资料等等。

FBI 和 CSI 在 2002 年对 484 家公司进行了网络安全专项调查，调查结果显示：超过 85% 的安全威胁来自公司内部、有 6% 来自内部未授权的存取，有 4% 来自专利信息被窃取，有 3% 来自内部人员的财务欺骗，而只有 2% 是来自黑客的攻击，在损失金额上，由于内部人员泄密导致了 60565000 美元的损失，是黑客所造成损失的 12 倍。这组数据充分说明了内部人员泄密的严重危害，同时也提醒人们应加强网络内部安全建设。建立起有效的事前预防、事后追究机制成了单位内部的当务之急。

## 2 如何建立一个可信并可控的内部网络

面对内部网络安全的严峻形势，建立一个基于监测、发现、制止、响应、责任追究的管理与技术防范机制显得尤为必要和突出，通过将监控和审计手段有机结合，打破以往审计系统主要针对日志记录事后追查的局限性，为及时阻止危及内部网络安全的违规事件发生、实时监控内部人员的违规操作、规范敏感信息和机密数据的存储和转移方式，可采用一些方便实用的技术手段和工具。因此，如何建立一个可信并可控的内部网络，成为摆在所有内网所有者和管理者面前的值得深思的课题。

要建立可信的内网，第一步是解决非法节点接入问题。现代化的楼宇布线为接入网络提供了便利，同时也带来了问题。外来人员可以很轻松的接入内部网络，访问或盗取内网上的核心资源或敏感信息，甚至对内网发动攻击。只有在非法节点接入后的第一时间发现并进行报警，并对非法节点进行隔离或阻断，才能有效地予以应付。然而，仅仅防范非法接入是不够的。即使是允许接入内网的计算机，在被有意无意地修改了 IP 地址后，也会导致网络运行异常，影响其他节点或重要服务器的运行等后果。对于这种情况，需要网络监控体系能第一时间发现并报警，在必要的情况下，对这些节点进行隔离或者阻断。在做到上述两点后，该节点仍不能保证是可信的。因为一台没有及时打上最新补丁、更新病毒数据库的计算机是整个网络防护的弱点，极易遭受病毒攻击或被黑客利用作为入侵的跳

板。因此，对合法接入网络但未达到防护标准的计算机进行访问范围的控制成为必然的选择。

即使建立了可信的内网仍不能高枕无忧。内部人员违章、大意、玩忽职守仍然可能导致严重的后果。必须采取各种手段把网络控制起来，降低人为操作的风险。包括以下手段。

### (1) 非法外联监控

一旦发现不通过正常路由访问外网的内网主机，及时报警，短开违规计算机与内外网的连接。

### (2) 运行软件监控

一旦发现内网主机未运行必须运行的软件或运行了禁止运行的软件，及时报警并杀死违规软件进程。

### (3) 运行设备监控

根据需要控制内网主机安装使用各种移动存储或传输设备，包括光驱、软驱、U 盘、串口、Modem、红外接口等。

### (4) 网络拓扑发现

动态扫描更新网络的逻辑拓扑和物理拓扑，显示子网划分和连接情况，能够直接关闭或启用交换机端口。

### (5) 服务性能监控

24 小时全天候监视重要服务器和网络服务的性能，发送异常信息。对于访问服务器资源的各种行为，进行实时监控和事后记录。

## 3 技管并用，确保网络安全

在内网安全管理中，除了采用技术措施之外，还应制定有关规章制度，这对于确保网络安全、可靠运行将起到十分有效的作用。规章制度作为一项核心内容，应始终贯穿于系统的安全生命周期。网络的的安全管理制度应包括：确定安全管理等级和安全管理范围、制订有关网络操作使用规程和人员出入机房管理制度、制定网络系统的维护制度和应急措施等。具体来说，为保证系统安全须从以下几方面规划。

物理与环境保护，包括：物理访问控制，建筑物安全，供电、供水、空调等公用设施的保证，设备安全，数据安全等五个方面。

针对不同的系统故障或灾难，制定突发事件的应急计划，并进行针对性的培训和演练。

- 在维护过程中对应用程序的版权、来源、

文档、测试进行规划和评估。

- 为保证数据完整性与有效性，需考虑系统的备份与恢复措施，计算机病毒的防范与检测制度，数据文件和统计数据的校验制度，系统日志文件的实时监控及异常停机处理等问题。
- 文档管理：包括软硬件、政策、标准、过程和相关的系统、支持系统的描述以及备份措施、突发事件对策、用户和操作员的说明等内容。
- 制定完整的规章制度，构建安全管理平

台，定期进行网络系统安全教育与培训。

网络安全是一个系统的、全局的管理问题，网络上的任何一个漏洞，都会导致全网的安全问题，我们应该用系统的观点、方法，分析网络的安全及具体措施。必须从网络、计算机操作系统、应用业务系统甚至系统安全管理规范、使用人员安全意识等各个层面统筹考虑。内网安全问题在安全体系中是至关重要的环节，解决内网安全问题必须从规划内网资源、规范内网行为、防止内网信息泄密等多方面入手，构建有效的安全管理机制，这样才能真正做到整个网络系统的安全。

#### 参考文献（略）

#### 作者联系方式

通信地址：北京市西三环北路一号武警总部网管中心

邮政编码：100089

联系电话：13801207052

# 建立联合作战可信网络构想

马献章 陈军 滕明贵

**摘 要:** 随着诸军兵种联合作战走进战争的历史舞台, 支撑联合作战的物质基础——信息网络也将从封闭的专用网络发展成为诸军兵种共用的公用网络, 网络世界的安全正在冲破传统信息安全框架的束缚。本文通过建立联合作战可信网络架构体系, 把内容边界防护、内网防护、主机防护、接入防护进行整合, 实现对联合作战信息网络的可信扩展以及完善的信息安全保护, 有效提升联合作战信息网络的整体安全防御能力。

**关键词:** 可信网络; 联合作战; 信息安全; 网络安全

## 1 前言

随着诸军兵种联合作战样式走进战争的历史舞台, 支撑联合作战的物质基础——信息网络也将从封闭的专用网络发展为诸军兵种共用的公用网络。虽然完善的联合作战信息网络构成目前尚未有准确的定义, 但可以肯定它将是包括诸军兵种专用和公用网络在内的一个纵横交错、包罗万象的繁杂体系, 几近涵盖作战应用的各个方面, 是一个崭新的网络世界。在这个的网络世界中, 分布在诸军兵种的多系统必将进行融合或互操作, 这种融合或互操作会造成多种技术体制的冲突与矛盾, 这种新的矛盾与冲突必然带来新的安全问题; 并且, 由于多系统融合或互操作而产生的安全问题要远远大于各单一系统安全问题的总和。美国信息化咨询委员会认为: 信息安全状况越来越糟, 打补丁、堵漏洞的方法不是有效的解决方案, 应从边界防护的模式中吸取惨痛的教训, 重新考虑安全问题, 在危险的世界中建立可信系统。我军也不例外, 过去的信息化建设, 大多在具有我军特色的编制体制框架下进行, 各军兵种在信息化的过程中, 针对其所面临的安全问题与应用需求, 配置了各种各样的安全产品, 构建了不同程度的基于信任管理、身份管理、脆弱性管理以及威胁管理等安全管理子系统, 初步实现了从单一安全产品到面向具体安全问题的集成化的安全解决方案的过渡。但是这些安全产品和安全解决方案是针对其特定需求的, 彼此间缺乏协作和沟通, 无法在联合作战信息网络中实现网络安全的整体防御。各个安全子系统就像是构成了“木桶理论”中纵向的木板, 由于各木板之间没有紧密地耦

合, 使得板间缝隙成了安全问题的关键所在。如何构建一个主动的、全体系的安全保障体系, 从根本上解决联合作战带来的新安全问题, 已经成为全军亟待解决的一个热点难点问题。本文通过建立联合作战可信网络架构体系, 构筑一个具有行为监管、行为认证、行为控制、行为对抗能力的有序、可信的安全体系, 将诸军兵种网络安全资源进行有效整合、管理与监管, 既保护已有的投资, 发挥已有安全设备的整体效能, 又实现联合作战信息网络的可信扩展以及完善的信息安全保护, 从而达到有效提升网络整体安全防御能力的目的。

## 2 可信计算概念的提出及其在国内外的的发展

“可信”可以追溯到 20 世纪 70 年代, 是一个历史悠久的话题, 它的发展要从容错计算说起。容错计算的研究与发展, 从 1971 年第一届国际容错计算会议 (FTCS-1) 开始, 进而发展到软件容错和网络容错。1995 年, 在第十五届国际容错计算会议 (FTCS-15) 上, IEEE Fellow、A·Avizienis 教授等人提出了可信计算 (Dependable Computing) 的概念, 此后, IEEE 的许多专家开始致力于可信计算的研究。

2000 年 12 月, 由美国卡内基梅隆大学和美国国家宇航局 NASA 以及 IBM、HP、Intel、微软等著名企业发起, 成立了可信计算联盟 (TCPA, Trusted Computing Platform Alliance), 此组织又于 2003 年 3 月改组为可信计算组织 (TCG, Trusted Computing Group)。TCPA 和 TCG 的出现形成,

使可信计算从学术界走向产业界，全球 IT 行业几乎所有的著名公司都加入了 TCG 这一组织。该组织不仅考虑信息的秘密性，更强调了信息的真实性和完整性，而且更加产业化和更具广泛性。TCG 确定的任务：定义、发展并推广开放的硬件可信计算和安全技术标准，其范围涵盖硬件模块、软件界面、跨平台、外围及各种装置等。目前，TCG 成立了多个工作小组，试图将其制订的规范推广到大量相关装置领域。2002 年 7 月，微软于公布了 Palladium 的“可信赖计划”，提出了未来十年的可信计算战略目标，并于 2003 年将其更名为下一代安全计算基础（NGSCB），强调可信计算在数字产权管理方面的应用。Intel 为支持微软的 Palladium 计划，2003 年 9 月推出了 LaGrande 技术，2004 年 12 月推出了使用该技术的 Prescott 新一代奔腾处理器。欧洲于 2006 年 1 月启动了名为“开放式可信计算（Open Trusted Computing）”的研究计划。微软新推的操作系统 Vista 不仅全面支持 TPM（Trusted Platform Module），并且其主要安全特性也以 TPM 作为其必备的硬件基础。微软 Vista 的推广与普及，将进一步促进 TPM 在 PC 中的标配进程。

在我国，可信计算研究起步较早。2000 年，国家密码管理委员会办公室开始立项研究可信计算技术。此后，2004 年 6 月，武汉瑞达公司就推出了国内首款自主研发的具有 TPM 功能的可信安全计算机；同年 12 月，天融信公司推出了可信安全管理平台和可信安全系统平台；2005 年 1 月，国家信息安全技术化标准委员会 WG1 组专门成立了可信计算工作小组。2005 年 4 月，联想、兆曰科技基于可信计算技术的 PC TPM 安全芯片产品正式推出，尔后联想开天 M400S、清华同方超翔 4800 及长城世恒 A/S 系列安全 PC 产品纷纷问世。“十一五”规划及“863”计划均将“可信计算”列入重点支持项目，并有较大规模投入。2005 年初，我国正式成立了可信计算标准工作组。2006 年 2 月，国务院公布的“国家中长期科学和技术发展规划纲要（2006—2020）”，提出了发展“高可信网络”的自主创新目标。目前，索尼和华硕不约而同采用了兆曰技术的 TPM 芯片，已经成为近来安全的最大卖点，我国从事可信计算技术研发的单位虽然不多，但效果已经相当显著。

## 3 联合作战可信网络的概念

### 3.1 “可信”概念的定义

可信计算的思想源于社会，其基本思想是在计算机系统中首先建立一个信任根，再建立一条信任链，一级测量认证一级，一级信任一级，把信任关系扩大到整个计算机系统，从而确保计算机系统的可信。

在网络世界中，安全的主要要求是保证计算可信、连接可信和应用可信。“可信”一词包括的含义非常广泛，根据中国安全产业分会的定义，它是一个包括 19 个平台的“可信网络世界”。在 X.509 中的定义是：“当第二个实体按着第一个实体的期望行为时，第一个实体可假设第二个实体是可信的。”在可信计算平台（TCP，Trusted Computing Platform）中的定义是：“总是达到预定目的的预期行为”，这里的“总是”二字强调了使可信具有时间连续性和统计概率的意义。在《软件行为学》中的定义是：“可信性是考察行为预期性的满足，这种预期性满足是在多主体多行为范畴内，实现对行为的性质、行为输入输出、行为过程、行为的属性等方面符合必须遵守的要求、约定、规定、规则、法律满足性认识与评价。行为的可信性还表现在发生行为预期和实际结果之间差距的认识、把握、控制、调整 and 改变。”

早期的可信概念是“授权可信”的概念，反映在美国国防部可信计算机系统评测标准（TCSEC）中，是“只看身份和权限，不看行为表现”，表现在保密性、完整性和可用性定义中；现代的可信概念是“既看身份与权限，又看行为表现”，体现在 TCPA 以及中国信息安全商会与天融信公司联合推出的相关概念定义上。“可信”由最初的“授权可信”发展为“行为可信”，最终落实在行为可信上。

### 3.2 “可信”与“安全”概念的区别

“安全”，侧重于考虑对用户信息资源的安全保护与服务能力的增强，并提供切实可行的安全产品，这是传统安全厂商所致力的工作目标。“可信”，则是为了建立用户对于信息系统的支撑平台（硬、软件系统）与安全保护系统能够正确处理与切实保护其信息资源能力的信心，且这种信心是建



立在对信息系统支撑平台及其安全保护系统中的行为进行监管的基础之上的。

传统的安全概念，是建立在“第三方安全保障承诺”基础上的安全，用户无法对安全保障能力进行预知和评估。基于“可信”的安全新理念，则把网络与系统中行为与内容的监管能力作为基础，为用户提供了考察其信息资源处理系统的支撑平台，以及安全保障机制的行为可信性的能力，使用户能够掌控信息资源处理过程中的安全状况，并能够有效规避可能的风险。后者强调了“第三方的功能和服务能力承诺”与“用户监管能力”的结合，对于用户来说具有来自于自己评判的实际意义，可以作为用户“自我安全保障能力”的体现。

3.3 联合作战可信网络的定义

可信网络架构不是一个具体的安全产品或一套针对性的安全解决体系，而是一个有机的网络安全全方位的架构体系化解决方案，强调实现各厂商的安全产品横向关联和纵向管理。TCG 对可信网络的定义是：如果网络中的行为与结果总是预期和可控的，那么网络是可信的。笔者认为，在联合作战信息网络中，具备了以下三个特征的网络，才能认为是可信的联合作战信息网络。

- 网络中的行为和行为中的结果总是可以预知与可控的。
- 网内的系统符合指定的安全策略，相对于联合作战安全策略是可信的、安全的。
- 联合作战诸军兵种、各作战集团、作战部队的端点系统能够动态接入，具备动态扩展性。

这个定义，可以通过在网络与系统上，针对联

合作战诸军兵种、作战集团军、作战部队、作战要素指挥、控制、保障、训练、管理等业务与技术的行为和行为结果提供行为控制、行为监管、行为认证、行为管理和行为对抗的充分能力，并建立相应的体系，维护网络的可信性。

联合作战可信网络主要解决的问题是边界威胁、内网威胁、主机威胁和接入威胁问题，重点考虑利用网络监管系统来解决联合作战网络范围内诸军兵种、作战集团、作战部队、作战分队的资源使用者及其活动的可信性问题，这种可信性是相对于整个联合作战网络资源的拥有者或应用者而言的。联合作战可信网络的研究，其最终目的是为了提高系统或网络资源的有效利用，保障系统或网络用户对指挥、控制、保障、训练、管理等业务应用的可信性。

4 联合作战可信网络的体系架构及安全模型

4.1 联合作战可信网络的体系架构

联合作战可信网络体系架构（Combined Operations Trusted Network Architecture—COTNA）是一个通过对诸军兵种现有网络安全设备和网络安全子系统的有效整合和管理，并结合可信网络的接入控制机制、网络内部信息的保护和信息加密传输机制，实现全面提高网络整体安全防护能力的可信网络安全技术体系。该体系主要从图 1 所示的几个视角来考虑联合作战网络整体的防御能力。

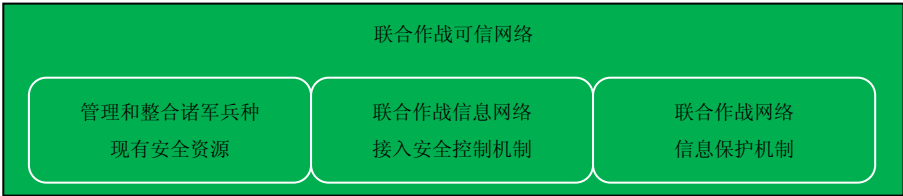


图 1 联合作战可信网络体系架构

在图 1 所示的体系架构中，**管理和整合诸军兵种现有安全资源**，从全局角度对网络安全状况进行分析、评估与管理，获得全局网络安全视图；通过制定安全策略指导或自动完成安全设施的重新部署或响应。**联合作战信息网络接入安全控制机制**，用

于构筑联合作战可信网络的安全边界，通过对可信终端系统的接入控制，实现其可信网络的有效扩展，并有效降低不可信终端系统接入网络所带来的潜在安全风险。**联合作战网络信息保护机制**，用于强化对联合作战网络资源的保护，解决联合作战诸

军兵种信息系统间的互通和互操作。

4.2 COTNA的安全模型

COTNA 主要包括联合作战可信安全管理系统（COTSM，Combined Operations Trusted Network Security Management System）、联合作战网关可信代理（COGTA，Combined Operations Gateway Trusted Agent）、联合作战网络可信代理（NTA，Combined Operations Network Trusted Agent）和端

点可信代理（PTA，Point Trusted Agent）四部分，从安全管理系统、安全产品、网络设备和端点用户等四个安全环节确保安全性与可信性，最终通过对用户网络已有的安全资源的有效整合和管理（如图 2 所示），以及基于可信代理（COPTA、CONTA 或 GTA）的可信网络安全接入机制，实现联合作战“可信网络”的动态扩展，增强联合作战信息网络内部信息及信息系统的等级保护，防止最终用户敏感信息的泄漏。

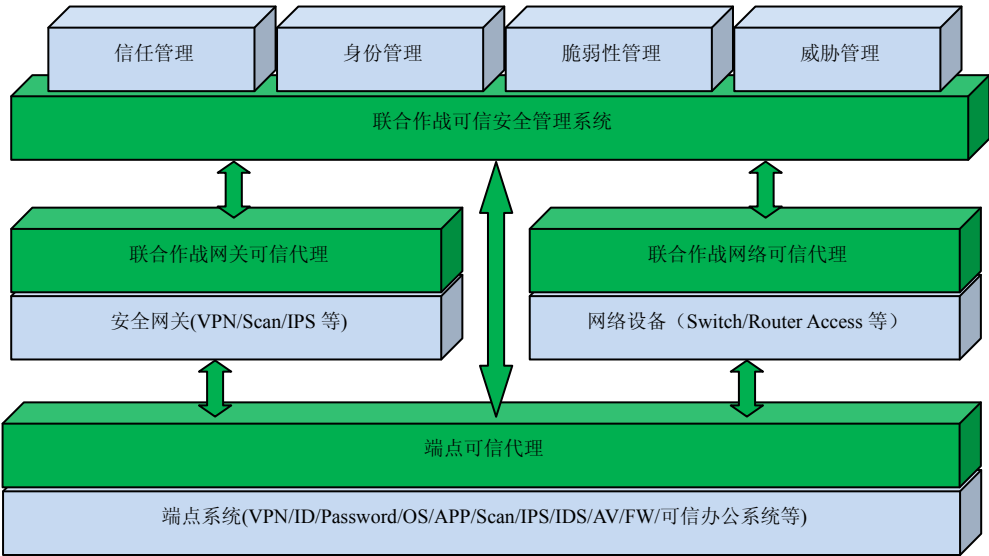


图 2 联合作战可信网络体系架构的安全模型

COTNA 对用户网络安全实施全面的、系统的、集中的安全管理，改变了以往针对某一安全事件所采用的安全管理模式，各安全产品之间实现了真正的关联，大大地节省了资源，实现了六个转变（一是使安全从被动防护到主动管理的转变；二是从单一的授权控制模式到授权控制和行为、内容的可信性并重模式的转变；三是从面向局域网络到面向超大规模网络环境的转变；四是从单一的安全责任到责任和效益并重的转变；五是从面对威胁或脆弱性到面对安全能力的转变；六是从安全性要求到可信性要求的转变），既可使联合作战“可信网络”安全应用范围无限拓展，又能极大地满足信息等级保护的要求，从而确保多层次的积极防御和综合防范。

5 联合作战可信网络体系架构的核心机制

COTNA 是在诸军兵种现有安全资源基础上的有效整合与管理，广为熟知的安全机制不再赘述。

本文重点讨论体系中新引入的安全机制以及用于安全资源整合的相关机制：COTSM、联合作战信息网络接入安全控制机制以及联合作战网络信息保护机制。

5.1 COTSM

COTSM 处于整个可信网络安全体系的核心位置。它通过对网络中各种设备（包括路由设备、安全设备等）、安全机制、安全信息的综合管理与分析，对现有安全资源进行有效管理和整合，从全局角度对网络安全状况进行分析、评估与管理，获得全局网络安全视图；通过制定安全策略指导或自动完成安全设施的重新部署或响应；从而全面提高整体网络的安全防护能力。

在 COTSM 中，安全事件管理、风险管理以及安全策略配置管理是网络安全管理系统实施安全机制整合的核心。

5.2 联合作战信息网络接入安全控制机制

联合作战信息网络接入安全控制机制主要是基于“可信代理”的安全机制，结合终端系统的认证、评估子系统来实现对接入联合作战可信网络的终端系统、用户进行认证/授权控制，只有通过了用户身份鉴别以及工作终端系统安全状况评估后，用户使用的终端系统才能够接入到动态的联合作战

网络中（如图 3 所示）。这种机制，能够有效地避免联合作战信息网络中因不可信终端系统接入所带来的潜在风险。这种机制中的可信代理，就像各军兵种各作战要素的安防中心，自主地完成所负责的区域的安全监管。依据所处的位置和功能，可信代理可分为端点可信代理（PTA）、联合作战网关可信代理（COGTA）以及联合作战网络可信代理（CONTA）三种类型。

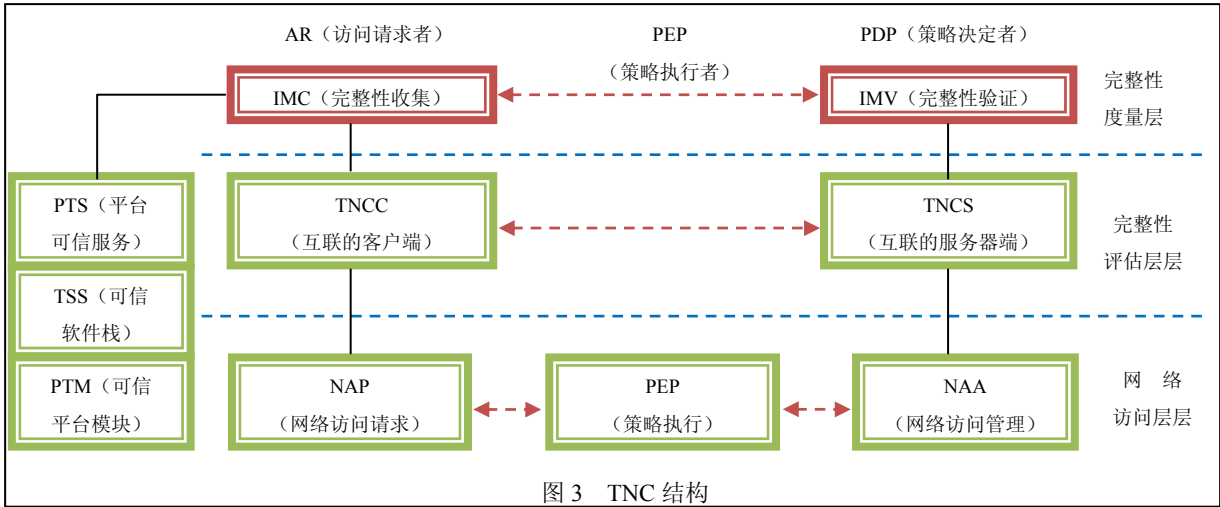


图 3 TNC 结构

5.2.1 PTA

PTA 工作在桌面系统中，用于采集待接入联合作战信息网络的终端系统的安全状况信息和终端操作用户的认证信息，并负责与位于网络接入设备上的 CONTA 或位于安全网关系统上的 COGTA，建立安全通信通道，而采集到的信息将通过可信的通信通道传送到网络接入安全控制机制的认证、评估子系统，来确定终端系统的可信与否。

此外，PTA 还需要提供终端安全应用的集成接口，用于采集不同安全应用的特征信息。

5.2.2 COGTA

COGTA 作为联合作战信息网络接入安全控制系统的组成部件之一，工作在安全网关系统上，处于 PTA 与端点安全状况评估子系统之间，主要具有设备定位信息、端点的监控以及策略下发、与 COTSM 安全通信以及安全应用信息交互等功能。

5.2.3 CONTA

CONTA 作为联合作战信息网络接入安全控制系统的组成部件之一，工作在网络接入设备上，处

于 PTA 与端点安全状况评估子系统之间，主要具有设备定位信息、端点的监控以及策略下发、与 COTSM 安全通信以及安全应用信息交互等功能。

此外，为了避免端点系统在可信端点接入后，人为破坏可信端点的安全策略配置、或者因可信网络安全策略的动态调整，使得在线端点系统的安全策略不满足可信网络的要求，在联合作战信息网络接入安全控制系统中还应具有“保信”（Keep Trusted）机制，具体思路是：由接入安全控制系统的认证、评估子系统周期性向所辖的可信端点进行周期轮询，要求进行端点安全状况的重新评估。策略如下：对于评估通过的，则可信端点的安全操作权限不变；对于不符合安全策略的，则降低该端点对网络的安全操作权限，通知修补系统，并拒绝访问相关区域。修补完成后，重新进行端点安全状况评估，通过后提升访问权限；对于 PTA 不响应的，则视为不可信端点，降低用户访问权限，禁止访问联合作战信息网络。

5.3 联合作战信息网络信息保护机制

联合作战信息网络信息保护机制，重点关注联

合作战信息网络内部重要信息的保护,以确保这些数据在存储、使用以及传输过程中的安全。并且通过控制联合作战信息网络内部用户访问外部时的安全策略检查机制以及外出信息的检查机制来避免敏感信息的外泄,从而保证联合作战信息网络内部信息的机密性和可信性。相关的技术包括:信息保护的安全模型、信息的可信传输机制、用户的身份鉴别与授权机制、违规网络外联检测与监控以及外出信息的信息流控制机制、内容过滤机制等。

## 6 结束语

今天的环境是网络无处不在,网络的环境是漏洞、攻击和病毒也不处不在,即使像美国这样充分

拥有互联网知识产权的国家,其国防部和联邦调查局核心网络也不能幸免。作为支撑联合作战的物质基础——信息网络,将直接影响到一个国家的安全,无疑不能构筑在这种安全失控的网络之上。可信网络思路的出现,带来了网络机制的原创机遇。

“国家中长期科学和技术发展规划纲要(2006—2020)”指出:“中国要在激烈的国际竞争中掌握主动权,就必须提高自主创新能力……”。国家信息化专家咨询委员会委员沈昌祥院士建议:目前我国信息安全建设正处于一个关键时期,发展可信计算战略具有非凡意义。我国在可信计算领域起步不晚,水平不低,我们应当抓住机遇,建立我军联合作战新的信息安全体系,在全球新军事革命中抢占有利先机。

## 参考文献

- [1] 《新一代安全及 NCI 理念》 QNS 工作室 南相浩 屈延文
- [2] 《发展高可信网络实现网络机制创新》 信息产业部通信科技委委员 嵇兆钧
- [3] 《从终端安全技术的发展谈脆弱性安全到结构性安全的演进》. [http://www.i170.com/user/falcon/Article\\_61974](http://www.i170.com/user/falcon/Article_61974)
- [4] 《可信终端成就安全体系》 [http://cio.cdw.com.cn/research/info/htm2004/20040613\\_1340T.asp](http://cio.cdw.com.cn/research/info/htm2004/20040613_1340T.asp)
- [5] Department of Defense Computer Security Center. DoD 5200. 28-STD. Department of Defense Trusted Computer System Evaluation Criteria[S]. USA: DOD, December 1985.
- [6] Trusted Computing Group. TCG Specification Architecture Overview [EB/OL]. [2005-03-01]. [https://WWW.Trustedcomputinggroup.org/groups/TCG\\_1-0-Architecture Overview.pdf](https://WWW.Trustedcomputinggroup.org/groups/TCG_1-0-Architecture%20Overview.pdf).
- [7] Intel Corporation.LaGrande Technology ArchitecturalOverview[EB/OL]. E2005-05-01]. <http://www.intel.com/technology/security/>.
- [8] Microsoft . Trusted Platform Module Services in Windows Longhorn [EB/OL]. [2005 — 04 — 25] . <http://WWW.microsoft.com/resources/tpm/>.
- [9] Patel J, Teacy W T, Luke, et al. A Probabilistic Trust Model for Handling Inaccurate Reputation Sources [C]//Trust Management, Third International Conference, iTrust 2005. Berlin Heidelberg: Springer, 2005: 193—209.
- [10] Beth T, Borcherding M, Klein B. Valuation of Trust in Open Network[-C]//Proc oy the European Symposium on Research in Security (ESORICS). Brighton: Springer—Verlag, 1994: 3-18.
- [11] 屈延文. 软件行为学[M]. 北京: 电子工业出版社, 2004. Qu Yanwen. Software Behavior[M]. Beijing: The Electronic Industry Press. 2004 (Ch) .

## 作者联系方式

通信地址: 四川省成都市北较场军区信息化工作办公室

邮政编码: 610011

联系电话: 028-86681332 86681302 86681328

# 全面贯彻落实科学发展观努力构建我军信息安全保障体系

史正祥 张建辉

**摘要:** 面对军队信息化发展过程中对信息安全的迫切需求以及我军信息安全保障能力的不足和面临的挑战,必须尽快建立军事信息安全保障体系,全面提高我军信息安全保障能力。本文结合当前我军信息安全保密工作现状,以科学发展观为指导,认真分析了我军信息安全保密工作面临的严峻形势,指出了存在的问题和不足,提出了构建我军信息安全保障体系的基本对策,为促进和保障军队信息化建设快速、健康、协调的发展提供参考。

**关键词:** 科学发展观;信息安全;保障体系;对策

军事信息安全保障体系是实施军事信息安全保障的法制、组织管理和技术等层面有机结合的整体,是军事信息安全的基本组织部分,是保证军队信息化顺利进行的基础。随着军队信息化建设的飞速发展,各项军事活动对信息和信息系统依赖性越来越强,军事信息安全保密工作不断暴露出的问题日益突出,特别是美、台等对我实施全方位侦察窃密和渗透,使我军事信息安全保密工作呈现出新的特点规律,面临着严重的威胁。如果不解决好信息安全的问题,不做好保密工作,直接影响和制约我军作战能力的提升。我们要以胡主席和军委关于加强军队信息安全保密工作的重要指示为指导,全面贯彻落实科学发展观,努力构建我军信息安全保障体系,促进和保障军队信息化建设快速、健康、协调的发展。

## 1 当前我军信息安全与保密面临的严峻形势

当今世界,信息已成为重要的战略资源,信息控制能力已成为国力、军力的重要体现,信息的争夺空前激烈,我军事信息安全面临前所未有的严峻挑战。

### 1.1 敌对势力的侦察窃密活动十分猖獗,使我军事信息面临现实的失泄密威胁

当前,窃密技术无奇不有,窃密手段无孔不入,窃密活动无处不在。长期以来,我敌对势力一直通过派遣侦察机、侦察船,发射侦察卫星,以及

在我周边建立数以百计的电子信号侦收站,猖狂地对我实施全天候、全方位和全频谱的信息侦察。据我相关部门透露,我东南沿海的部分军事目标已被准确无误地收录到外军的情报数据库中。一些发达国家和地区还利用经济合作、贸易谈判、文化交流、探亲旅游等多种渠道,采用腐蚀拉拢、金钱利诱、心战策反等多种手段,千方百计套取我机密情报。从近年来发生的数次特大间谍案中,我们应清醒地认识到,窃密与反窃密、渗透与反渗透、策反与反策反等隐蔽战线的斗争越来越激烈,信息安全保密难度越来越大。

### 1.2 信息化战争呈现出新的特点规律,使我军事信息安全保密工作难度空前增大

信息的流动性和信息网络的开放性,决定了军事信息安全保密工作将随着信息化进程的不断推进,逐步向陆、海、空、天、电、磁多维立体空间拓展,不断呈现出新的特点规律。军民界限模糊,军事信息安全与保密工作面临着军民一体的综合威胁。信息作战不再仅限于正规军人的行动,每个芯片都可能是一种潜在的武器,每台计算机都有可能成为一个有效的作战单元,一台计算机、一条电话线加一个解调器就能发动全球信息攻击。信息攻防活动可以不知不觉地渗透到各个领域,而且无时无刻不在进行。平战时域渐趋模糊,军事信息安全保密工作受到长期不间断的威胁。信息时代的战争建立在信息社会基础之上,具有传统战争形态所没有的新特点,很难有“平时”和“战时”的一定之规,特别是在信息领域的对抗行动更是难有“平时”和“战时”之分。使得军事信息系统受到的威



胁是不间断的，这给军事信息安全保密工作提出了新的挑战。战场界限模糊，军事信息安全保密工作面临着诸多性质不定的多层次威胁。未来作战很难有前方、后方之说，信息对整个战争起到控制、牵引和决定作用，军事信息安全保密工作贯穿于战争的全方位、全环节，熔铸于作战的全时域、全过程，渗透到每个作战单元、每件武器装备，使我军军事信息安全保密面临多重威胁。

### 1.3 自主可控核心技术匮乏和对国外的依赖性增强，使我军信息系统安全根基存有严重隐患

我军信息化建设自主核心技术匮乏，信息系统关键核心部件依赖于国外受制于他人，信息基础设施比较脆弱，信息安全根基存有严重隐患，随时处于被干扰、被监视和被欺诈等多种信息安全威胁中。一些发达国家利用其在信息技术领域的垄断地位和优势，在出口的计算机芯片、软件系统中隐藏“木马”和嵌入指定的病毒程序，可将计算机的所有信息全部返回其情报部门。而我军信息安全科研基础条件相对薄弱，信息安全综合技术水平还处在以信息加密为主，逐步向系统安全过渡的初级阶段，尚未形成完整、可靠、具有自主产权的安全防护技术体系和装备体系，所采取的一些防护措施和所使用的安全设备，大多技术水平不高，数量不足，不能完全满足实际需要。

## 2 我军信息安全保密工作呈现的突出问题

近几年，在军委、总部的正确领导下，军事信息安全保密工作意识逐步强化，各项措施正在加强，已经取得了较为明显的成绩，为保障和促进军队信息化建设发挥了重要作用。但由于我军信息化起步较晚，基础较差，军事信息安全与保障工作的历史较短，经验不足，技术手段较为落后，还不能很好地适应军队信息化建设的快速发展，主要表现在以下几个方面。

### 2.1 缺少信息安全保密的高级技术和管理人才，部分单位和官兵信息安全保密意识不强

当前，我军还没有建立起适应信息化和信息安

全保密工作发展需要的多类人才的培训体系，各单位各部门大部分都是靠抽调相近专业、甚至与信息安全保密专业无关的人员从事此项工作，缺少相对稳定的队伍。致使本单位本部门出现一些问题，也不能及时得到有效的解决。部分单位和官兵信息安全整体意识仍然不强，在网络建设上，我们的保密手段相对滞后，许多军事信息尚未得到密码的有效保护，重“通”不重“密”的现象依然存在。军事信息安全保密系统建设管理上还存在着一些带倾向性的问题，有的只看到它给工作带来的方便，看不到信息处理不安全会带来的严重危害和后果；有的单位和个人消极保安全，不愿用，不敢用安全保密系统，在网络建设中存在着重建设轻防护，重使用轻保密的现象。

### 2.2 信息安全组织领导体制和运行机制不够健全

目前全军涉及信息安全与保密工作的领导管理有多个机构，没有形成高效统一的协调工作机制。有关部门职责分工还完全适应新形势任务要求，存在条块分割、职能交叉、多头管理、分工不明确、制度不健全和责任不到位、协调力度不够大等问题。特别是在跨领域、跨部门协调任务越来越重的情况下，现行的领导管理体制已不能适应信息安全与保密工作建设指导、运行管理和作战指挥的需求。

### 2.3 安全核心技术研发开发比较落后

目前，我军在信息安全技术领域具有自主知识产权的产品很少，对关键技术机理的掌握也很缺乏，采用的基础硬件和操作系统、数据库等系统软件大部分依赖国外产品，在这些产品中可能存在预置的后门与漏洞。用于构建网络的软、硬件，基本上都是国外引进的，信息安全保密技术受到国外的严密封锁。现有科研开发力量十分薄弱，从事专门研究信息安全的人员非常少，在核心软硬件技术的开发领域更难有大突破。部分信息安全设备缺乏规范化接口标准，系统兼容性、移植性和可靠性差，战技术性能指标低。一些成熟的安全保密装备未能成建制、成系统地配置，无法形成完整的安全防护体系。密码基础设施的建设和管理经费还没有完全纳入正常渠道，有的单位尚未落实密码保障机构和人员，难以支撑信息安全保密系统的正常运行，长

此以往,势必严重影响军事信息安全与保密工作。

## 2.4 基础网络的整体防护能力还比较弱

我军现在运行的大部分网络和信息系统不同程度地存在着安全隐患,安全体系不健全,失泄密和被攻击情况时有发生。军事信息系统的安全设备大多相对孤立的分散装备在网络上,每类设备有自己的一套管理系统,这些管理系统虽然对各处的安全设备实施管理,但都没有提供统一的安全管理接口,安全管理人员无法对网络安全系统的整体情况加以全面监视和管理,无法实现一体化的动态防御功能,使我网络安全防护的整体效能相对较弱。

## 2.5 信息安全法规和标准建设滞后

目前,我军针对信息安全保密的法规标准尽管出台了一些文件和法规,但还缺少综合性和基础性,有些法规不能很好适应军事信息安全与保密工作的要求,不能适应新形势的需要,内容重复、交叉现象普遍,可操作性不强。军事信息安全标准质量不高,指导性不强,标准体系建设缺乏系统性。致使在我们实际的工作中,保密规定在落实上存在很多漏洞和死角,安全管理特别是内部管理还比较松懈。还有些单位不严格按章办事,规章制度形同虚设,落实得不好。

# 3 构建我军信息安全保障体系的基本对策

新的历史形势下,我们要按照军委、总部有关加强我军安全保密工作的指示精神,全面贯彻落实科学发展观,充分认识做好军事信息安全保密工作的极端重要性,加大工作力度,下大力解决制约和影响我军信息安全保密工作的突出问题,紧紧围绕“打赢信息化条件下局部战争”这一战略目标,全面提高军事信息安全防护能力,加大保障和促进军队信息化健康发展。

## 3.1 加强军事信息安全与保密工作的组织领导,建立高效的领导管理体制

军事信息安全与保密工作是一项动态的、复杂的系统工程,涉及军队建设的各个领域,涉及到各

个部门,直接影响和制约我军作战能力的提高,必须加强对军事信息安全与保密工作的组织领导,建立起高度权威、统一、顺畅的管理体制。建议在全军信息化领导小组内设立信息安全保障小组,在全军信息化工作办公室建立专家组织实体,负责跨部门、跨领域的信息安全与保密工作的协调。建议建立军内外信息安全与保密工作联席工作机制,定期通报情况。调整细化总部有关职能部门任务职责,明确协作要求,建立分工明确、协调有力、密切配合的工作机制。

## 3.2 加大经费投入,构筑具有自主产权的信息安全防护支撑平台

在未来信息化作战中,依靠引进的信息安全产品,是靠不住和信不过的,只有走独立自主的发展道路,研发具有自主知识产权的信息安全保密设备,才能在战争中立于不败之地。当前,迫切需要加大经费投入,大力发展专用芯片、专用操作系统、安全数据库以及安全网络协议等技术的研究,努力开发自主的核心技术,切实提高安全防护的底数。要积极开展量子密码、实用编码和标准算法等技术的研究,提高密码对多形态信息高速处理的适应性。要不断发展信息安全设备的检测和监控技术,努力完善信息系统安全防护手段,为促进我军信息化建设的良性发展,奠定坚实的安全技术基础。

## 3.3 加快信息安全人才培养,建设专业的信息安全保障队伍

应把培养信息安全专业人才作为实施信息安全战略的重中之重,确立培养和发展战略,并纳入全军人才发展的战略规划,按照满足需求、适度超前的原则,分层次、分阶段实施专业培训,以逐步培养造就一支“高精尖”信息安全专业人才群体。首先,完善以院校为主渠道的人才培养机制。在相关院校建立培训基地,设立信息安全专业学科,制定培养计划,为我军源源不断地培养、输送和储备信息安全人才;二是借助社会办学机构培训军队信息安全人才;三是加强对外交流,使现有信息安全人才拓宽视野,增强素质。同时,在培养人才、引进人才的基础,还应建立起人尽其才、才尽其用、暖心留人的新机制,为人才充分施展才干提供一个宽阔的平台。注重从制度上解决人才的使用与保留问

题,努力为信息安全人才提供良好的工作条件和广阔的事业发展空间,为建设一支强大而稳定的信息安全专业队伍提供制度保障。

### 3.4 加强军事信息安全法规标准研究,完善信息安全保障法规体系

在信息安全领域,技术十分关键,但并非万能,必须依靠十分严格的行政管理和技术管理,才能使技术措施发挥应有的效能。当前,应集中力量,健全完善信息安全法规框架,全面规划信息安全标准化工作,形成具有我军特色的信息安全标准体系。信息安全涉及到军队建设的各个方面,不可能由某一机构独立完成,必须建立与信息安全任务相适应的管理机构和职能部门,才能协调好整个军事信息安全与保密工作,才能针对信息安全的特点及时发现信息安全方面所存在的漏洞和各种潜在威胁,并及时做出反应。建立和健全信息安全方面的法律和法规,并加大执法和监督的力度,确保信息

安全方面有法可依,有法必依。

### 3.5 尽快制定军事信息安全与保密工作的应急处置预案,强化处突能力建设

定期检查,及时发现系统存在的安全隐患,预测可能出现的各种情况,并以此为依据,制定相关应急预案,以便在系统遭受攻击、破坏或出现故障时,能在较短的时间内恢复使用。对重要数据要及时备份,防止丢失;对遭受损失破坏的后勤信息系统,要有备用系统及时接替工作;对重要信息保障渠道,要建立必要的迂回信道,避免一处受阻,整体瘫痪;要广泛采用新的技术手段,及时修复受损信息,保证信息的完整性和真实性。依托有关技术平台和已有的应急技术支撑机构,整合资源,构建军事信息安全与保密工作应急响应体系,初步具备信息网络空间中突发事件的发现分析、通报预警、处置恢复和追踪反制能力。

### 参考文献

- [1] 侯喜贵.《军队信息化建设研究》.北京:解放军出版社,2002
- [2] 《胡主席关于国防和军队建设贯彻落实科学发展观重要论述摘编》总参谋部政治部宣传部,2007
- [3] 戴清民.《科学发展观与军队信息化》.北京:解放军出版社,2007
- [4] 《中国信息化持续发展战略研究》.北京:科学技术文献出版社,2006
- [5] 《军队指挥自动化》杂志 2006 年合订本

### 作者联系方式

通信地址:武汉市解放公园路 45 号科研部

邮政编码:430010

联系电话:027-85968202



# 信息化系统抗电磁脉冲方法的研究

常海峰 徐筱麟 王小梅 温怀斌

**摘要:** 电磁脉冲 (EMP) 具有频带宽、峰值功率高、上升时间快等特点, 作为军用武器可以对各种信息化系统产生巨大的危害。它可以在一瞬间造成通信中断、控制失灵, 甚至使电子器件烧毁, 因此研究电磁脉冲对信息化系统的影响及其防护有着极其重要的意义。本文首先分析电磁脉冲对信息化系统的影响, 而后在此基础上提出了电磁脉冲的防护和加固方法。

**关键词:** 电磁脉冲; 时域有限差分法; 防护

## 1 引言

日新月异的信息技术以前所未有的力量推动着整个世界的发展, 同时也使电子战、信息战成为未来战场的主要样式。电子战的其中一个主要任务就是利用各种电子战武器, 在关键时刻、关键地点和主要进攻方向上, 对敌方的  $C^4ISR$  系统<sup>[1]</sup> (指挥、控制、通信、计算机和情报、监视、侦察系统) 系统和精确制导武器以及隐身目标的薄弱环节实施集中的、高强度的电子攻击, 造成敌方雷达迷茫、通信中断、武器失控、指挥失灵, 从而瓦解其战斗力<sup>[2]</sup>。电磁脉冲武器正是可以完成这种战斗任务的典型电子战武器。然而对于己方来说, 电磁脉冲的有效防护也是保持不败的必要条件。本文就是在分析电磁脉冲对信息化系统影响的基础上初步探讨了信息化系统的防护与加固措施。

## 2 电磁脉冲对电子系统的影响

随着微电子技术的迅猛发展, 以大规模集成电路为核心的信息系统已广泛应用于  $C^4ISR$  系统的各个领域。这使得信息系统的集成度愈来愈高, 存储量愈来愈大, 速度和精度也不断提高, 而系统的工作电压却只有几伏, 工作电流也只有微安级, 故系统对外界干扰极其敏感, 这使得信息化系统对电磁脉冲的承受能力几乎为零。电磁脉冲会通过缆线耦合传输到内部电路, 也可通过屏蔽体表面的孔缝耦合进内部的敏感电路, 使其系统功能暂时或永久性的失效。为了更清楚说明电磁脉冲所产生的危

害, 本文依次在高空核电磁脉冲 (HEMP) 及正弦调制的高斯脉冲环境下, 运用时域有限差分法 (FDTD) 计算并仿真了缆线及孔缝所感应的电磁脉冲能量。

1966 年, K.S.Yee 提出了时域有限差分法的基本原理。之后二十年, 它的研究进展缓慢, 只在电磁散射、电磁兼容领域有些初步应用。到 20 世纪 80 年代后期以来, 随着吸收边界条件的改善、网格剖分技术与并行计算技术等方面的发展与进步, 使得 FDTD 成为电磁场问题最原始、最本质、最完备的数值模拟方法<sup>[3]</sup>。在 FDTD 基础上制作的仿真程序, 对广泛的电磁场问题具有通用性。图 1、2 就是利用 FDTD 的基本原理分别给出了传输线与孔缝的最简单的计算模型。

### 2.1 缆线的耦合仿真与分析

在图 1 的模型设置中假设缆线半径为 1cm、距地面高 5cm、缆线两端无任何接地、大地电磁参数取  $\sigma_g = 0.01 \text{ S/m}$ 、相对介电常数  $\epsilon_r = 5$ , 入射电场为 HEMP, 可用公式表示为:

$$E(t) = E_0(e^{-\beta t} - e^{-\alpha t}) \quad (1)$$

式 (1) 中  $E_0 = 5.25 \times 10^4 \text{ V/m}$ ,  $\alpha = 4.76 \times 10^8 \text{ s}^{-1}$ ,  $\beta = 4.0 \times 10^6 \text{ s}^{-1}$ 。最后再根据安培环路定理可计算出缆线感应电流为:

$$I = \oint (\vec{n} \times \vec{H}) dl = \oint \vec{H} \cdot d\vec{l} \quad (2)$$

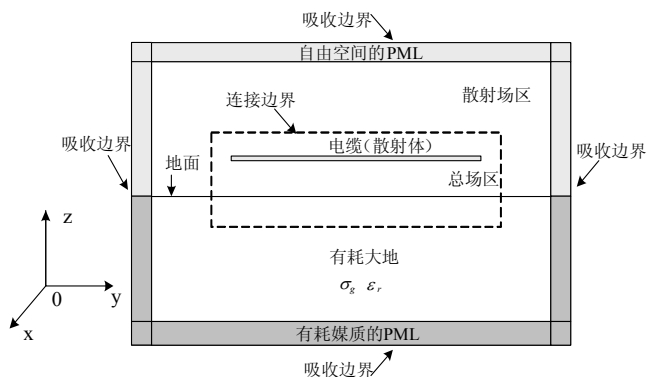


图1 传输线计算模型设置

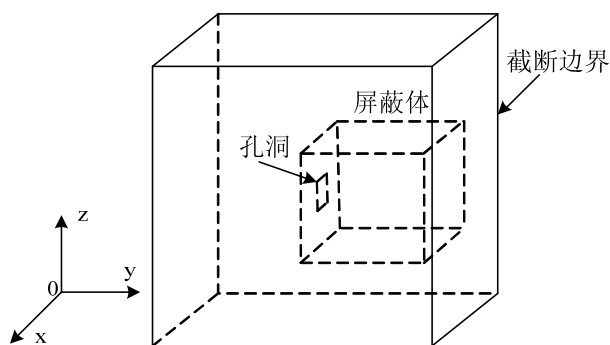


图2 孔缝的计算模型设置

其中积分路径为缆线表面的圆周。仿真结果如下。

从图3~图5可以发现，暴露在HEMP环境下的有限长近地缆线存在以下规律。

1) 图3表明缆线外导体的感应电流随缆线长度的增加而增大，通常在HEMP条件下缆线外导体可以感应几百甚至上千安培的电流。

2) 从图4可看出所在缆线位置的不同外导体所感应的电流也有所不同，且越靠近缆线中间点感应电流越大。

3) 图5是随HEMP入射角不同，导致地面反射的情况也有所不同，进而缆线外导体的感应电流产生变化，当HEMP垂直于缆线辐射时缆线的感应电流最大。

另外，缆线外导体的感应电流也会随架设高度、入射仰角、大地电导率等因素而变化<sup>[4]</sup>，从总体上可以看出在HEMP环境下，与电子设备相连的缆线会耦合出非常高的电流，这对于电子设备而言是无法承受的。

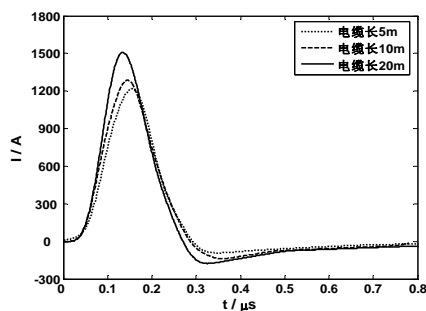


图3 随电缆长度的变化

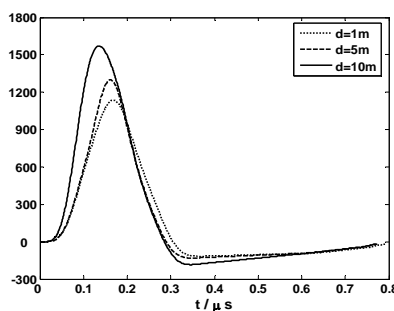


图4 随电缆上位置的变化

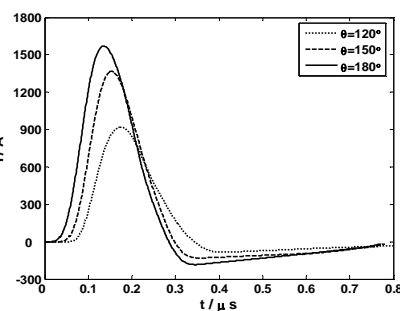


图5 随入射角θ的变化

## 2.2 孔缝的耦合仿真分析

在图2的模型设置中假定屏蔽体为边长15cm的正方体，而孔洞为边长3cm的正方形。平面波激励源由连接边界处加入，本文所采用的正弦调制的高斯脉冲，其表达式为：

$$E_i = E_0 \cos(2\pi f t) \exp\left[-\frac{(t-t_0)^2}{\sigma^2}\right] \quad (3)$$

式(3)中 $f=3.0\text{GHz}$ 为入射波载频， $E_0=1.0\times 10^5\text{V/m}$ ， $t_0=1.5\times 10^{-9}\text{s}$ ， $\sigma=7.0711\times 10^{-10}$ 。其中z方向线极化平面波沿y方向传播，即垂直于孔洞面入射。仿真结果如下。

正弦调制的高斯脉冲从孔洞面垂直入射，经过孔洞使得高斯脉冲高频分量耦合进入屏蔽体内部，

而低频分量则被截止，图6是孔中心内1cm处的电场 $E_z$ 随时间变化的曲线，可以看出，脉冲初次经过测试点时电场 $E_z$ 的值很大，比较接近波源电场值，当激励源脉冲结束后，屏蔽体内的振荡电磁波会再通过孔洞辐射到屏蔽体外，这样导致孔内场值不断减小。由图7可看出，电磁脉冲进入屏蔽体后，屏蔽体中心点耦合的场能量首先是不断增加的，当激励源脉冲过后，屏蔽体内的电磁波会在体内来回反复振荡，并通过孔洞向外不断辐射能量，这会导致屏蔽体内的耦合能量逐渐减少，这个过程会持续较长一段时间。总的来说，如此之大的电磁脉冲耦合能量会对大规模的集成电路和半导体元件造成极大的破坏。

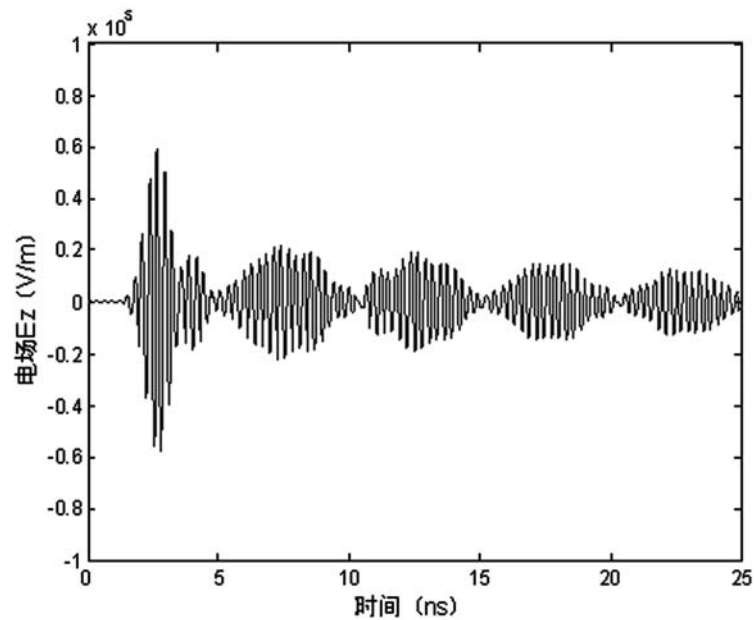


图 6 孔中心内 1cm 处电场  $E_z$  的时域图

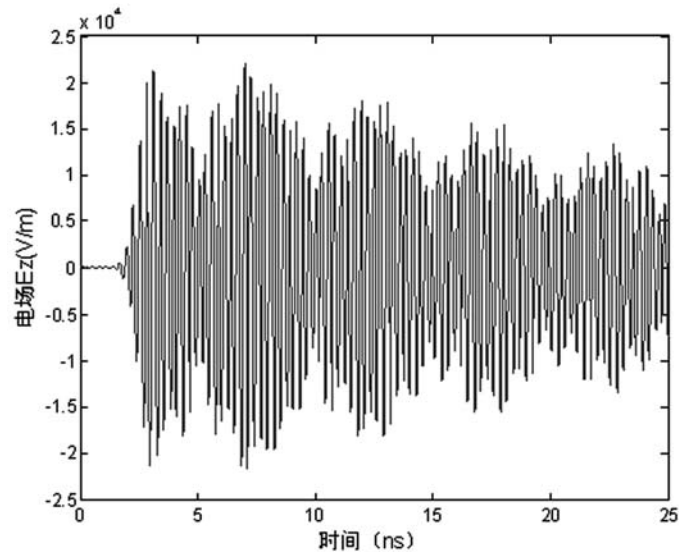


图 7 屏蔽体中心处电场  $E_z$  的时域图

### 3 EMP的防护

针对电磁脉冲的特性及危害，我们通常可以采取接地、屏蔽和滤波的方法来避免电磁脉冲能量进入电子系统，从而使其衰减到设备能够承受的程度。该节将根据上述方法逐一对电磁脉冲的防护进行介绍。

#### 3.1 屏蔽

##### 3.1.1 缆线的屏蔽

EMP 作用下的一根几十米长的近地缆线，可

以感应上千安培的电流或上万伏的高压。这么高的能量对与缆线相连的电子、电气设备及系统的安全运行构成了严重的威胁，因此我们必须采取屏蔽措施。金属丝编织层，软导管，金属硬管或者螺旋形缠绕的高导磁率的带条，都可以用作缆线的屏蔽层。在固定台站或人防工程中，用无缝的硬金属管作为缆线的外层屏蔽可以达到很好的屏蔽效果，但采用这种方法对战时机动性能存在着很大的隐患。对于编织电缆，当频率在  $10^6 \sim 10^7 \text{Hz}$  以下时，屏蔽效能与利用金属管所做的实壁缆线区别不大，但当频率再高时，转移阻抗迅速上升，编织电缆的屏蔽效能就会大大下降。虽然也可通过增大编织密

度、改变缆线倾角和覆盖范围加以改善，但效果仍达不到预期目的。因此，我们可以采用组合屏蔽的方式，这样可在整个频谱范围内提供最大的屏蔽效果，并可增加一定的机动性能。组合屏蔽方式利用100%覆盖范围的金属箔层（例如铝箔）与具有机械强度和低直流阻抗等优点的网状屏蔽相结合，以此屏蔽方式便可实现野战通信的电磁防护要求。组合屏蔽应注意各层屏蔽材料的表面不能相互连接在一起，其间应留出一个用空气或介质材料填充的小空间带，但这无疑会增加缆线制作的成本和复杂度。

另外一个良好的缆线屏蔽，不仅指缆线本身的屏蔽，还应包括屏蔽层在缆线两端的端接状况以及所用连接器的形式。缆线屏蔽层和电器装置的屏蔽

体（外壳）要有可靠的电接触，同时缆线屏蔽层和电器装置间的缝隙要尽可能的小。

### 3.1.2 孔缝的屏蔽

为了提供实用的服务，电器装置的屏蔽体不可能采用完全的封闭，因此一个实际的电磁屏蔽体上总有许多导电不连续的因素，图8是一个典型的机箱，由图可见机箱装配面处的接缝、通风冷却孔、显示窗口和器件调谐孔等都是导致耦合电磁场能量的因素。正是这些因素的存在，使屏蔽体的屏蔽效能很难达到预期的程度，也正是这些因素使屏蔽体的设计成为一个较为复杂的问题。所以，对屏蔽体加固是电子系统防护的一个极为重要的方面。

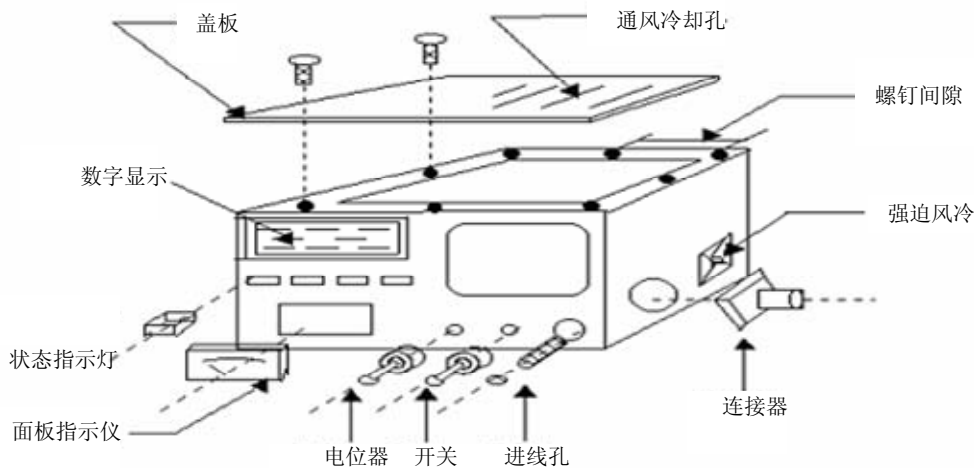


图8 典型机箱示意图

对这些孔缝进行屏蔽可供选择包括以下几个方案。

- 1) 采用连续焊接、调整紧固钉间距或改变缝隙结构以提高接缝的电磁密闭效果；
- 2) 采用隔离舱将一些外露器件与设备内部的电路隔离开，使外部的干扰不能侵入到屏蔽体内部；
- 3) 对重要的元器件及灵敏元件进行屏蔽，对所有进入设备的导线进行滤波；
- 4) 对于通风口，可在相同的面积地情况下把较大的通风孔改成孔径较小的多孔阵列<sup>[5]</sup>；
- 5) 对于显示窗口要使用加细导线编制网的透明屏蔽材料；
- 6) 调谐轴与调谐孔之间所存在间隙可采用截止波导管。

## 3.2 接地

缆线屏蔽层接地与否对电磁环境下的屏蔽缆线来说是非常重要的，屏蔽层接地是为防止缆线因受电磁干扰，而影响缆线本身或与其相连的设备正常工作的一种有效方式，通常屏蔽缆线接地可分为单点接地和多点接地。当金属屏蔽层采用一端接地时将带来下列问题：电磁感应产生的过电流或过电压沿屏蔽层流动时，金属屏蔽层在不接地端会出现很高的冲击电压，在缆线绝缘外护层不能承受这种过电压的作用而损坏时，会导致缆芯出现多点接地，形成环流或者烧毁与其相连的设备。因此在电磁防护中缆线屏蔽层应尽量采用多点接地，这样既可保证缆线之间没有电位差，同时也可将感应电流迅速从多点接地处释放电流，从而避免了感应电流耦合进入与其相连的设备。

由于缆线感应的瞬时电流值过高，接地电阻也会暂时升高数倍以上。为了更好地对缆线进行防护，我们还要尽量减小接地电阻。在城市自然条件下，接地体应尽量与混凝土中的钢筋、埋地的金属水管等相连以降低接地系统中的接地电阻；在野战条件下，我们可人为改变接地土壤性质或增加接地体的数量来降低电阻。

3.3 滤波

为了防止外部电磁脉冲进入电子系统，需要在被保护的物体之间加入滤波器，以吸收电磁脉冲中剩余的能量，保证电子系统中每个敏感元件两端的电压或电流不超过其所能承受的范围。通常滤波器不能承受强电磁脉冲所产生的峰值电压，故而滤波器通常要与一些保护电路或元器件配合使用，这些保护器件包括：火花隙放电器、气体放电管、变阻器和半导体器件（例如雪崩二极管）。

火花隙放电器通常是把电压加以限制，然后用滤波器把内部电路与外界电磁脉冲隔离起来。当遇到能量较大的 EMP 时，可以采用瞬态抑制二极管

(TVS)，TVS 具有响应速度快、瞬态功率大、漏电流小等特点。TVS 能以  $10^{-12}$ S 量级的速度将两级的高阻抗变为低阻抗，并可吸收数千瓦的浪涌功率，使两极电压箝位于预定值<sup>[6]</sup>，但一旦超过它的功耗极限，TVS 就会损坏，引起 EMP 滤波器失效。通常在选用时，应确定被保护的电路的最大支流，电路的额定标准电压以及高端容限。另外 TVS 并联使用时，可以允许更大的电流通过；而串联使用时，总电压为各个 TVS 的压降之和。气体放电管常用于泄放暂态过电流和限制过电压，由于气体放电管的极间绝缘电阻很大，寄生电容很小，所以对高频电子线路的电磁防护具有明显的优势。但不足之处在于其放电时延较大，动作灵敏度不够理想，对于上升陡度较大的电磁波难以有效地抑制，因此常用于多级保护电路中的第一级或前两级。对于金属氧化物压敏电阻器（MOV），它能承受比 TVS 更大的冲击能量，但是每经过一次 EMP 冲击，它的性能会下降，经过多次冲击后，MOV 会丧失对 EMP 的防护能力。图 9 给出了一种三级保护器件在电路中的应用。

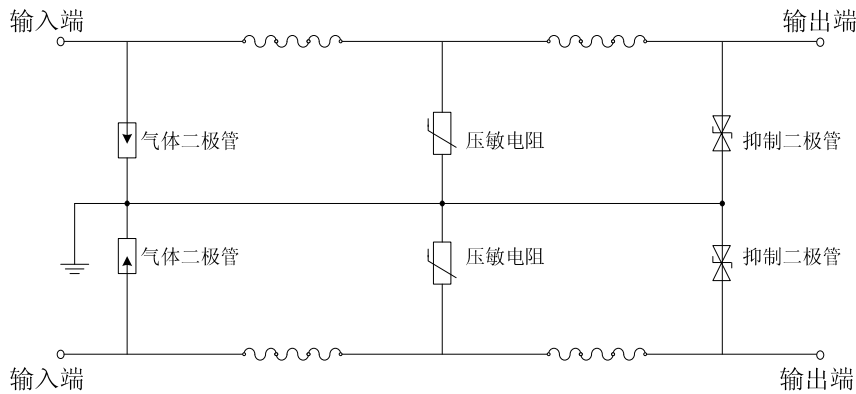


图 9 三级保护器件在电路中的应用示意图

总之在设计电子系统之前，我们应该按照国、军标要求，充分考虑内部电路中电子器件的敏感度，并根据可能遇到的电磁脉冲环境，合理加入保护电路，以做到在未来战场中万无一失。

4 结论

随着信息时代的到来，以大规模集成电路为基

础的电子系统逐渐成为信息战场上电磁脉冲武器的主要攻击对象。因此做好有效的电磁脉冲防护，才能更好的提高我军战斗力，进而使我军在未来信息战场上立于不败之地。

参考文献（略）

作者联系方式

通信地址：解放军理工大学通信工程学院研究生 2 队      邮政编码：210007      联系电话：13115012856

# 军队信息安全保障及技术对策

付仕平 解家宝 徐飞

**摘 要:** 文章阐述了信息安全保障的概念及技术对策。重点介绍了三种关键技术, 密码技术, 数字水印技术及信息隐藏技术, 分析了其系统构成及各种算法。

**关键词:** 信息安全保障; 密码技术; 信息隐藏; 数字水印

## 1 引言

军事信息网络同普通网络一样, 需要对网络及边界进行保护, 以防止因为敌人的入侵而造成网络的瘫痪, 同时, 还需要对信息的内容进行保护, 防止敌方获取我方机密信息, 从而进一步对我方军事系统进行打击。围绕信息和信息系统而展开的信息作战行动将贯穿作战全过程, 夺取制信息权将成为整个作战活动的重心之一, 这就导致信息安全问题凸现。解决好战场信息安全问题, 为信息和信息系统提供可靠的信息安全保障, 将是赢得信息作战胜利的基础和关键。

## 2 信息安全保障的概念

信息保障的概念首先由美国军方提出, 为区别于“信息安全”概念, 同时体现出继承性, 国内常采用“信息安全保障”概念。所谓“信息安全保障”, 是指“保证信息和信息系统的保密性、完整性、可用性、可控性和不可否认性的信息安全保护和防御过程。它要求加强对信息和信息系统的保护, 加强对信息安全事件和各种脆弱性的检测, 提高应急响应能力和系统恢复能力。由该定义可以看出, 信息安全保障已不再局限于传统信息安全对信息和信息系统的保护, 而是更强调重视系统的入侵检测能力、系统的事件反应能力以及系统在遭到入侵引起破坏后的快速恢复能力。这样, 保护、检测、反应和恢复就构成了信息安全保障具有动态反馈特点的四大环节。

## 3 信息安全保障的技术对策

### 3.1 密码技术

密码技术是保护信息安全的主要手段之一, 是保障信息安全的核心。通过数据加密, 变换信息的

表示形式来保护敏感信息, 使非授权使用者不能了解被保护信息的内容, 而知道密钥的授权用户可以解密加密信息以获取被保护信息的内容。密码技术不仅具有信息加密功能, 而且具有数字签名, 身份验证, 秘密分存, 系统安全等功能。所以, 使用密码技术不仅可以保证信息的机密性, 而且可以保证信息的完整性和正确性, 防止信息被篡改, 伪造或假冒。

#### 3.1.1 密码体制

一个密码体制是满足以下条件的五元组  $(P, C, K, E, D)$ : ① $P$  表示所有可能的明文组成的有限集 (明文空间); ② $C$  表示所有可能的密文组成的有限集 (密文空间); ③ $K$  表示所有可能的密钥组成的有限集 (密钥空间); ④对任意  $k \in K$ , 都存在加密法则  $e_k \in E$  和相应的解密法则  $d_k \in D$ 。并且, 对每一个  $e_k: P \rightarrow C$  和  $d_k: C \rightarrow P$ , 对任意的明文  $x \in P$ , 均有  $d_k(e_k(x)) = x$ 。

在以上各个条件中, 最重要的是条件④, 它保证了如果使用  $e_k$  对明文  $x$  进行加密, 则可使用相应的  $d_k$  对密文进行解密, 从而得到明文  $x$ 。

#### 3.1.2 Shannon保密通信系统模型

Shannon 于 1949 年提出了保密通信系统模型, 见图 1。

在图 1 中, 明文  $x$  被发送之前, 发送者和接收者之间使用的密钥要事先商定。即从对应得密钥空间  $K$  中选取一个特定的密钥。这个密钥经商定后必须严加保密。在 Shannon 称之为理想密码系统中, 密文的所有统计特性都与所使用的密钥独立。为此, 密码算法主要基于两个设计方法: 扩散和混乱。一般来说, 系统的保密性不依赖于加密体制或算法的保密, 而只依赖于密钥。

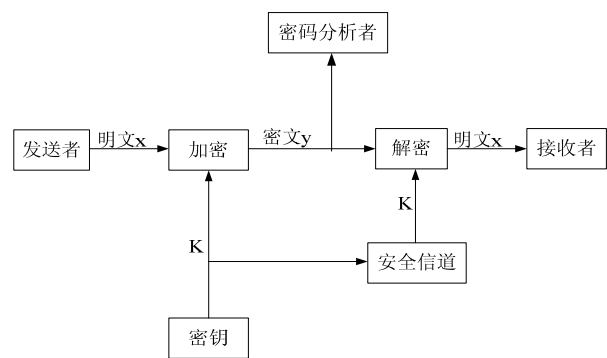


图1 Shannon 保密通信系统模型

3.1.3 密码算法分类

密码算法是密码技术的核心。目前，常用的加密方法有私钥密码算法和公钥密码算法，而混沌加密原理的出现为密码学提供了一种崭新的方法。

私钥密码算法也称对称密码算法。在对称加密系统中，加密和解密采用相同的密钥。这样对称密码算法的加解密速度快。但其缺点是：① 密钥的分发和管理非常复杂，代价高昂。② 不能用于数字签名。对称密码算法最著名的是美国数据加密标准 DES 和高级加密标准 AES。

公钥密码算法也称非对称密码算法。在这种算法中，加密密钥可以公开，而解密密钥必须是严格保密的。从解密密钥中可以很容易推出加密密钥，但是从加密密钥中却很难推出解密密钥。公钥密码算法的这种单向特性是基于陷门单向函数实现的。目前，密码学界已经提出许多公钥密码算法，如但 RSA、ECC、NTRU、背包体制、ElGamal 算法等，但影响最大的是 RSA 和 ECC 算法。

混沌加密不同于所有的传统算法，其根本的区别于这种加密方法所用的随机序列由混沌系统产生。一个混沌系统在混沌区内输出一个随机序列，将它作为密钥流去调制明文流，从而产生一个加密的密文流。采用混沌编码方式，利用混沌序列进行编码，在混沌序列的产生中已加入了舍入误差，混沌序列已不完全遵循非线性系统方程，因此较难通过神经网络等方法把混沌序列所遵循的方程重构出来。同时，密钥由系统方程、系统参数、系统初值、数据处理方式和编码方式等组成。即使破译者掌握了其中之一，要破译密钥也是非常困难的。

3.2 数字水印技术

所谓数字水印技术，是将数字、序列号、文

字、图像标志等版权信息嵌入到多媒体数据中，以起到版权保护、秘密通信、数据文件的真伪鉴别和产品标志等作用。简单地说，数字水印技术就是在多媒体数据中嵌入一段信息，嵌入的信息就是数字水印，是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，而且不影响宿主数据的可用性。

3.2.1 水印嵌入系统的结构

所有的水印系统至少包括 2 个模块：水印嵌入模块，水印检测及提取模块。原始图像经过知觉分析决定可以对某一像素的最大改变不会导致与原图像的明显区别。他需要考虑人类视觉系统的频率掩蔽特性，隐藏的信息与知觉掩蔽信号的作用，能实现保持图像修改的不可见的前提下，使嵌入的水印能量尽可能大。另外信息的扩张依赖于密钥,不具有密钥的人很难恢复隐藏的信息。最后将水印信号加入到原始图像，就得到嵌入水印的图像。

3.2.2 典型数字水印算法

根据数字水印的加载方法的不同，可分为两大类：空间域水印算法和变换域水印算法。较早的水印算法从本质上来说都是空间域上的，水印直接加载在数据上，有如下几种。

最低有效位方法（LSB）：这是一种典型的空间域数据隐藏算法。该方法是利用原数据的最低几位比特来隐藏信息。LSB 方法的优点是有较大的信息隐藏量，但采用此方法实现的水印很脆弱，无法经受一些无损和有损的信息处理。此外，如果确切地知道水印隐藏在第几位 LSB 中，则水印可以很容易地被擦除或绕过。

Patchwork 方法及纹理块映射编码方法：Patchwork 方法是一种基于统计的水印，其加载方法是任意选择 N 对图像点，在增加一点亮度的同时，降低另一点的亮度值。纹理方法映射将一块纹理映射至与其相似的纹理上去，视觉不易察觉。该算法的隐蔽性较好，并且对无损的 JPEG 压缩、滤波、扭转等操作具有抵抗能力，但仅适用于具有大量任意纹理区域的图像，而且不能完全自动完成。

文档结构微调方法：由 Brassil 等人首先提出了 3 种在通用文档图像中隐藏特定二进制信息的技术，水印信息通过轻微调整文档中的以下结构来完成编码：垂直移动行距、水平调整字距、调整文字特性（如字体）。基于此方法的水印可以抵抗一些

文档操作，如：照相复制和扫描复制，但也很容易被破坏，而且仅适用于文档图像类。

变换域水印算法是水印技术最初研究的热门问题,也是目前发展得比较成熟的领域。它具有鲁棒性强、隐蔽性好的特点。这类技术一般基于常用的图像变换，或基于局部或是全部的变换。比如：离散余弦变换（DCT）、小波变换（WT）、傅氏变换（FT 或 FFT）以及哈达马变换等。

这其中基于分块的 DCT 是最常用的变换之一。Cox 等人提出了基于图像全局变换的水印方法。该水印方案是对整个图像进行 DCT，然后将水印加载在预先决定的范围内的除去 DC 分量的低频分量上，水印则是由高斯分布的一实数序列组成，水印加载在 DCT 系数的强度上，即改变 DCT 系数的程度大小正比于相应的频率分量的信号强度。

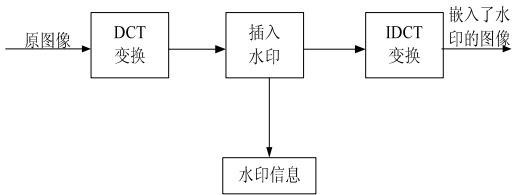


图 2 基于 DCT 变换的数字水印嵌入过程

3.3 信息隐藏技术

3.3.1 信息隐藏技术的含义

信息隐藏技术是将隐秘信息隐藏在其他媒体中，通过媒体的传输，实现隐秘信息的传递。它摆脱了信息加密的缺陷，可以在看似很正常的载体中嵌入信息，进行传递。信息加密所保护的是消息的内容。信息隐藏则不同，秘密信息被隐藏在表面看起来无害的宿主信息中，敌人无法判断他所监测的信息中是否含有秘密消息。信息隐藏的目的不在于限制正常的资料存取，而在于保证隐藏的信息不引起攻击者的注意和重视，从而减少被侵犯的可能性，在此基础上再使用密码学中的经典方法来加强隐藏信息的安全性，可以起到保护信息安全的作用。

参考文献（略）

作者联系方式

通信地址：安徽省合肥市黄山路 460 号 407 室电子工程学院研三队  
邮政编码：230037  
联系电话：0551—5767697

3.3.2 信息隐藏系统的构成

信息隐藏系统的构成通常可以用图 3 来表示，其中合成器用于将待隐信息通过密钥使用某种算法嵌入到遮掩消息中，形成外部特征与遮掩消息相同的隐写文档，该文档通过公开信道进行传输，接收到隐写文档的一方，通过与合成器相对的分离器，将待隐信息从隐写文档中分离出来。目前，通常用文字、图像文件、语音文件以及其他多媒体文件作为遮掩消息。

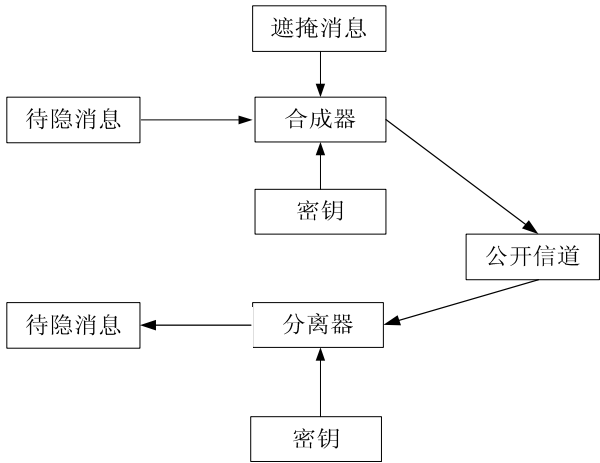


图 3 信息隐藏系统的构成

4 结束语

未来高科技战争中，不仅要夺取空中优势、海上优势，更重要的是夺取信息优势。信息是未来战争的重要资源，信息安全保障是取得信息战胜利的基础。然而，由于信息网络的国际化、全球化，使其面临的威胁来自各个角落，并在形式上呈现多样性。特别是军事信息系统，更是敌方首要的攻击目标。未来的战场是信息化的战场，不融入信息安全保障理念的军事信息网络建设，那就等于把控制自己“战马的缰绳”交给了敌方，终将受制于人。军事信息系统作为作战武器，必须把信息安全保障提到了战略地位，建立基于纵深防御的信息安全保障机制，才能在对抗中发挥最大效能。



# 军队信息安全保障体系建设初探

顾正义 孟娟 胡维益

**摘要：**随着军队信息化水平的提高，军队信息安全保障体系的建设已经到了非常重要的阶段。本文详细介绍了信息安全保障体系的 WPDRR 模型以及深层防御战略的核心思想，按照网络与基础设施防御、区域边界防御、计算环境防御、支撑性基础设施建设四个方面对系统建设进行了设计，最后阐述了信息安全保障体系建设需要的五个要素。

**关键词：**信息安全保障；WPDRR；深层防御战略

随着军队信息化建设持续快速发展，军队信息系统已经覆盖了部队的作战指挥、辅助决策、装备维护、后勤补给、卫星定位、精确制导、战场态势及日常办公各个方面。实践表明，一支军队的信息化水平越高，对信息系统的依赖性就越强，信息安全问题就越突出。信息安全问题已经成为一个事关军队现代化建设顺利进行和打赢未来高技术战争的全局性问题。我们必须瞄准世界信息技术发展趋势，努力构筑一个技术先进、管理高效、平战结合、安全可靠的信息安全保障体系，确保军队现代化建设和军事斗争准备的顺利进行。

## 1 信息安全保障体系模型

### 1.1 信息安全保障概念

我们所说的信息安全是指计算机信息系统安全，国际标准化组织（ISO）对计算机信息系统安全的定义是：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄漏。”

信息安全保障（IA-Information Assurance），其内涵已超出传统的信息安全保密，其定义是保证信息的机密性（保证信息不泄漏给未经授权的人）、完整性（防止信息被未经授权的人篡改，保证真实的信息从真实的信源无失真地到达真实的信宿）、可用性（保证信息及信息系统确实为授权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝服务，或为被恶意攻击者利用）、可控性（对信息及信息系统实施安全监控管理）、不可否

认性（保证信息行为人不能否认自己的行为）以及保证信息系统的可靠性。

### 1.2 信息安全体系的APPDRR模型

信息安全是一个动态的概念，APPDRR 模型是在进行详细的风险分析下，在整体的安全策略的控制和指导下，在综合运用防护工具（如：防火墙、身份认证、加密等手段）的同时，利用检测工具（如：漏洞评估、入侵检测等系统）了解和评估系统的安全状态，通过适当的反应将系统调整到“最安全”和“风险最低”的状态，并通过备份容灾手段来保证系统在受到攻击后的迅速恢复。

APPDRR 动态安全模型包含 6 个主要部分：Analysis（分析）、Policy（策略）、Protection（防护）、Detection（检测）、Response（响应）、Recovery（恢复），从安全体系的可实施、动态性角度，动态安全体系的设计充分考虑到风险评估、安全策略的制定、防御系统、监控与检测、响应与恢复等各个方面，并且考虑到各个部分之间的动态关系与依赖性。

### 1.3 信息保障的WPDRR模型

在 APPDRR 模型中，网络系统的四道防线是 PDRR（防护、检测、响应和恢复）。区别于传统的加密、身份认证、访问控制、防火墙、安全路由等技术，信息保障强调信息系统整个生命周期的防御和恢复，同时安全问题的出现和解决方案也超越了纯技术范畴。我们在原来 PDRR 前加上一个 W（Warning），用 WPDRR 这五个环节和人、操作（包括相关法律、法规、制度、管理等）和技术三

大要素来构成宏观的信息安全保障体系结构的框架。它构成了五种能力，即：预警能力、防护能力、检测能力、反应能力、恢复能力。因为信息安全保障不是单一因素的，它不仅仅是技术问题，而是人、操作和技术三大要素的结合。这样，信息安全就进入了有保障的体系，即信息保障的 WPDRR 模型。模型结构如图 1 所示。

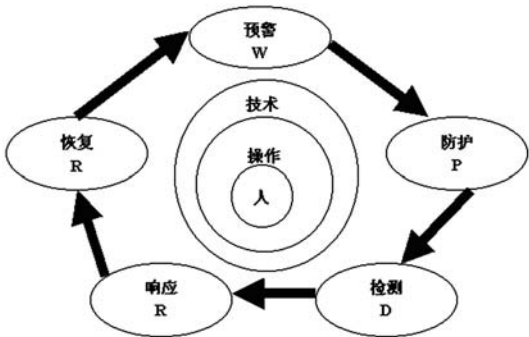


图 1 WPDRR 模型

1.4 深层防御战略

信息安全保障的核心思想是深层防御战略 (Defense in Depth)。所谓深层防御战略就是采用一个层次化的、多样性的安全措施来保障用户信息及信息系统的安全。如图 2 所示。

在深层防御战略中，人、技术和操作是三个主要核心因素，要保障信息及信息系统的安全，三者缺一不可；从技术上讲深层防御战略体现为在四个技术框架焦点域：网络和基础设施，区域边界、计算环境和支撑性基础设施等多个环节之中如何实现预警、防护、检测、响应和恢复 (WPDRR) 这五个安全内容。

深层防御战略的含义是多方面的，它试图全面覆盖一个层次化的、多样性的安全保障框架。深层防御战略的核心目标就是在攻击者成功地破坏了某个保护机制的情况下，其他保护机制依然能够提供附加的保护。

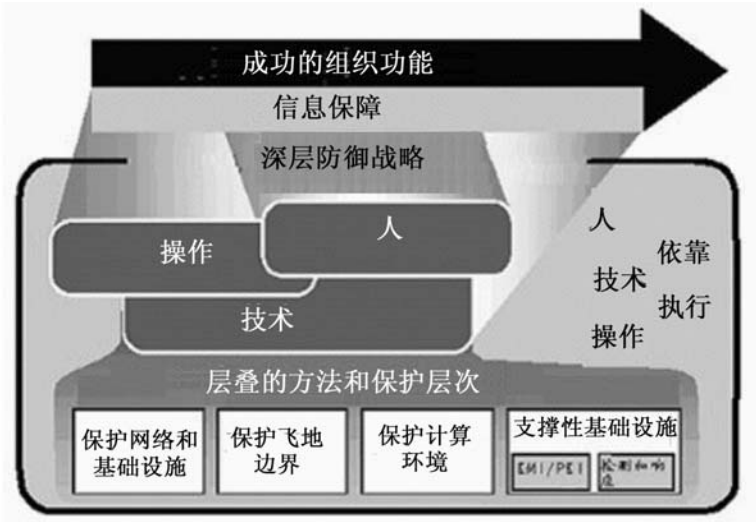


图 2 深层防御战略体系

2 军队信息安全保障体系框架设计

我们根据 IATF 所关注的四个技术框架焦点区域，并结合 WPDRR 模型和深层防御战略思想，对军队信息安全保障体系分四个部分进行设计。

2.1 网络与基础设施防御

网络和支撑它的基础设施是各种信息系统和业务系统的中枢，为用户数据流和用户信息获取提供了一个传输机制，它的安全是整个信息系统安全的

基础。网络和基础设施防御包括：保护各级网络和基础设施，对各级网络分别进行评估，确保它们得到适当的保护；通过动态路由、VPN 网络、骨干设备和链路的冗余、QoS 保障、网管系统以及物理防护来保障整个网络和基础设施的正常运行；维护信息服务，防止拒绝服务攻击 (DoS)；保护在整个广域网上进行交换的公共的、私人的或保密的信息，避免这些信息在无意中泄漏给未授权访问者或发生更改、延时或发送失败；阻止网络上所有不必要的通信，保证网络畅通等。

对军队信息系统来说，数据的安全交换和授权

访问是最基本的要求，所以必须保证网络及其基础设施能在无故障、不受外界影响的情况下稳定可靠地运行，不会由于安全设备的引入造成时延或数据流的堵塞，并保证所传输的数据不会被未授权的用户所访问。这就要求军队各部门在建立网络时要事先考虑到可能的业务类型和访问量等，保证建立的网络具有足够的带宽和良好的性能来支持这些服务和业务，并能有效抵抗恶意攻击。除了对网络和基础设施进行优化配置管理以外，各部门还应根据业务和信息的重要程度来进行网络隔离或建立虚拟专用网（VPN），从物理或逻辑上将业务网和公用网络实施隔离，使信息能在一个专用的网络通道中进行传递，这样能有效减少来自公用网络的攻击。

## 2.2 区域边界防御

根据业务的重要性、管理等级和安全等级的不同，一个信息系统通常可以划分多个区域，每个区域是在单一统辖权控制下的物理环境，具有逻辑和物理安全措施。这些区域大多具有和其他区域或网络相连接的外部连接。区域边界防御关注的是如何对进出这些区域边界的数据流进行有效的控制与监视，对区域边界的基础设施实施保护。

根据区域的安全等级在每个区域边界设置硬件或软件防火墙，对进出边界的数据进行策略控制；部署身份认证系统，对访问者进行身份认证；部署漏洞扫描与入侵检测机制，以提高对网络及设备自身安全漏洞和内外攻击行为的检测、监控和实时处理能力；设置防毒网关，防止病毒通过网络边界入侵应用系统。总而言之，要确保在被保护区域内的系统与网络保持可接受的可用性，并能够完全防范拒绝服务这一入侵攻击。

## 2.3 计算环境防御

在计算环境中的安全防护对象包括用户应用环境中的服务器、客户机以及其上安装的操作系统和应用系统，这些应用能够提供包括信息访问、存储、传输、录入等在内的服务。计算环境防御就是要利用识别与认证（I&A）、访问控制等技术确保进出内部系统数据的可控性、保密性、完整性和不可否认性。这是信息系统安全保护的最后一道防线。

在军队信息系统中，保护计算环境可以考虑以下方式：保护应用系统程序安全，包括使用安全的操作系统和应用程序；在关键服务器上部署主机入

侵检测系统和主机审计策略，以防止来自区域内部授权访问者或管理人员的攻击；部署防病毒系统，防止来自网络之外的病毒感染；使用主机脆弱性扫描系统，以减少主机漏洞，实现对主机的最优化配置；关键的配置文件或可执行文件实施文件完整性保护等。

## 2.4 支撑性基础设施建设

支撑性基础设施是一套相关联的活动与能够提供安全服务的基础设施相结合的综合体。目前纵深防御策略定义了两种支撑基础设施：密钥管理基础设施（KMI）/公钥基础设施（PKI）和检测与响应基础设施。KMI/PKI 涉及网络环境的各个环节，是密码服务的基础；本地 KMI/PKI 提供本地授权，广域网范围的 KMI/PKI 提供证书、目录以及密钥产生和发布功能。检测与响应基础设施中的组成部分提供用户预警、检测、识别可能的网络攻击、做出有效响应以及对攻击行为进行调查分析等功能。

就军队信息系统而言，需要建立一个用于管理全军网络的加密认证装置、VPN 设备等所有组件的密钥管理中心，对密钥的生成、备份、传递、分发、使用、更新、恢复和销毁进行统一的管理。同时要部署入侵检测系统、审计、配置系统，以提高系统的安全强度，保护数据的机密性、完整性和可用性。

# 3 建设军队信息安全保障体系需要的五个要素

## 3.1 权威的信息安全领导管理机构

信息安全是一个综合集成系统，它的规划、管理要求进行科学的、强有力的干预和导向。因此，必须突出该领导管理机构的权威性。目前，军队各部门各系统都有自己的专用网络，专用信息系统，大家各自为政，以计算机网络为主的信息安全管理更是涉及多个职能部门，应当将其统一归口到一个主管部门，或成立一个凌驾于各个职能部门之上的权威机构，并进一步强化其权限和职能，使其能从战略的高度来统揽全军的信息安全工作，实施重大决策，制定宏观政策，协调各方关系，统一进行管理，避免重复建设和物力、财力的浪费。

### 3.2 完善的法规制度和技术标准

健全的法规制度是信息安全保障体系的法制基础,也是依法进行信息安全管理依据和前提。应根据形势发展,借鉴国内外立法经验,结合部队实际,尽快建立一个权威性、操作性和系统性比较强的信息安全法规体系。

信息安全的技术标准也是安全保障体系建设的一个重要内容,虽然我国目前已经发布了一些国标和军用标准,但是还没有形成一套成熟的标准体系。只有技术标准确定了,信息安全产品的生产、信息系统建设和检测评估才能标准化、规范化;不同部门、不同厂家的产品和网络应用,才能兼容。

### 3.3 信息安全技术研究进一步加强

信息安全技术是具有对抗性的敏感技术,真正先进、核心的信息安全技术和产品是买不来的,因此军队要保障信息系统安全,必须加强对信息安全技术的研究,突出研究重点,将自主研究与合作研究结合起来,形成符合军队实际的良性研发机制。积极促进科研成果向战斗力转化,逐步形成具有军队特色的、先进可靠的信息安全技术装备体系。

### 3.4 高素质信息安全人才队伍

高素质的人才队伍是信息安全保障体系的智力支撑,在普及信息安全知识、提高官兵信息安全意识的基础上,要制定出信息安全人才发展战略,完善教育培养、引进和使用的机制,制定有利于人才成长的相关政策,努力建设一支专业精深、技管兼备、善于创新的高素质信息安全人才队伍。

### 3.5 完善的军队信息安全基础设施

信息安全基础设施是构筑信息安全保障体系的根基。军队的信息安全能否得到有效的保障,根本问题在于军队信息安全基础设施的完备程度。与道路、水、电等其他基础设施一样,比如需要用电的单位不一定都要建电厂。信息安全基础设施的建设也是如此,要使用证书不一定需要自己建立CA中心。通过完善军队信息安全基础设施,可以使提供的安全服务更加专业又节约成本。需要建设的相关设施包括:建立军队的信息安全管理中心,提供认证、授权、实施访问控制策略等服务;建立密码管理中心,提供各部门间互连互通密码配置、公钥证书和传统的对称密钥的管理,为信息系统提供密码服务;建立军队网络安全事件应急响应中心,对信息安全相关紧急事件进行专业响应;建立数据备份和灾难恢复设施;建立军队信息安全认证认可机构。

### 参考文献

- [1] 沈昌祥.《浅谈信息安全保障体系》. 信息网络安全, 2001.1
- [2] 袁丹洪, 欧阳剑雄.《大型政务网络系统信息安全保障体系研究》. 计算机与现代化, 2005.5
- [3] 丛友贵.《加速构建军队信息安全保障体系》信息安全与通信保密, 2002.11
- [4] 樊莉, 刘志勤, 赵玖玲.《构建军事信息系统安全体系的研究》. 网络安全技术与应用, 2005.10
- [5] 吴以四.《曲成义谈国家信息安全保障体系建设》. 信息系统工程, 2005.6
- [6] 国家 973 信息与网络安全体系研究课题组组织翻译,《信息保障技术框架》(3.0 版), 美国国家安全局发布, 北京中软件电子出版社, 2002.4。

### 作者联系方式

通信地址: 江苏省南京市黄浦路3号军区指挥自动化站

邮政编码: 210016

联系电话: 13813991344

# 移动存储介质安全管理机制的研究与实现

郭卫东 谢永强 王朝君 刘进

**摘 要：**分析移动存储介质安全管理的技术现状，针对移动存储介质安全管理机制的不足，提出使用安全标签对移动存储介质进行认证和访问控制的思想，进一步阐述安全标签的功能和判定流程，并基于日志型闪存盘实现该安全管理机制。

**关键词：**安全标签；认证标记；绑定标记；等级标记；日志型闪存盘

## 1 前言

目前，移动存储介质（移动硬盘、U 盘等）已得到普及应用，但越来越多的敏感信息存贮其中，给单位的信息资源带来相当大的安全威胁。如何安全有效地对移动存储介质进行管理已成为目前各单位亟需解决的问题之一。本文首先分析移动存储介质安全管理的技术现状，然后提出使用安全标签对移动存储介质进行认证和访问控制的思想，进一步阐述安全标签的功能和判定流程，并基于日志型闪存盘实现该安全管理机制。

## 2 移动存储介质安全管理机制研究现状

### 2.1 移动存储介质安全管理机制概述

现有移动存储介质安全管理系统大都采用 C/S 结构，由服务器端（Server）和客户端（Client）两部分构成。服务器端是安全管理系统的控制端，安装在管理主机上，主要工作是制定安全策略和对移动存储介质进行注册；客户端是被管理主机，在每台客户端主机上安装监控代理程序，主要作用是对移动存储介质进行认证和访问控制，并根据制定的安全策略封堵客户端主机的外设和端口。

### 2.2 现有移动存储介质安全管理机制存在的安全隐患

1) 部分管理系统采用的认证标记为终身不变的字符串，一旦该认证标记被截获或破解，则认证的安全性就面临巨大的威胁。

2) 认证域划分粒度不细，不利于单位信息流的控制。现有认证机制以管理系统所在单位为一个认证域，单位内注册移动存储介质可读写单位内任意一台客户端主机上的信息。这种情况导致主机内信息出口不唯一，一旦发生失泄密事件，不易定位相关责任人。

3) 只有身份认证，而没有采用访问控制机制，易出现越权访问的安全事件。依据现有管理系统的安全管理机制，移动存储介质一旦通过认证就可对客户端主机上信息进行任意读写，信息的保密性和完整性都将面临安全威胁。

4) 现有移动存储介质大多为被动的信息存储介质而无主动的控制代码，不能做到主动认证主机的真实性，而只能被动接受主机的认证，对于移动存储介质的安全存在一定的威胁。

## 3 移动存储介质安全管理机制的研究

### 3.1 安全标签的提出

针对现有移动存储介质安全管理机制存在的安全问题，提出安全标签（Security label）的概念。安全标签由认证标记（Authentication label）、绑定标记（Bind label）和等级标记（Rank label）三个分项组成，其中认证标记用来标识移动存储介质是否已在服务器端注册，绑定标记用来标识移动存储介质是否与插入的主机一一对应，而等级标记用来标识移动存储介质和所插入主机的安全级别的高低。在客户端监控代理程序时，将安全标签交由客户端监控代理程序保护，同时服务器端在对单位移动存储介质进行注册时将对应的安全标签写入其特定存储区域保护起来。安全标签的组成如图 1 所示：

安全标签	
分项名称	功能
认证标记	标识移动存储介质是否已在服务器端注册
绑定标记	标识移动存储介质是否与插入的主机一一对应
等级标记	标识移动存储介质与客户端主机安全级别的高低

图1 安全标签

### 3.4 等级标记概述

等级标记用来标识移动存储介质和客户端主机的安全级别，决定移动存储介质的读写控制。移动存储介质根据其使用者在单位内的职务分为绝密、机密、秘密和无密四个等级级别，从高到低对应等级标记的值可分别设置为 3、2、1、0，在管理系统注册移动存储介质时对其等级标记进行设置；客户端主机也根据它的使用者的职务分为绝密、机密、秘密和无密四个安全级别，在安装监控代理程序时指定该主机的安全级别。

### 3.5 判断流程的设计

移动存储介质在插入单位主机时需进行三个步骤的判断，即认证标记的匹配、绑定标记的匹配和等级标记的比较，具体又分为移动存储介质的判断和客户端监控代理程序的判断两个方面。因此，需要采用一种具有主动控制代码的移动存储介质才可完成以上判断步骤，在具体实现时我们采用的是一种日志型闪存盘，它具有主动控制代码并且可对其代码进行进一步的扩展，便于实现其他相关安全功能。监控代理程序在探测到有新的移动存储介质插入客户端主机时，首先要判断是否是日志型闪存盘，如果是则交由日志型闪存盘来做主动判断，否则监控代理程序根据单位的安全策略对移动存储介质的读写功能进行处理。日志型闪存盘与监控代理程序的判断流程分别见图2和图3。

### 3.2 认证标记概述

认证标记用于单位注册移动存储介质与单位客户端主机之间的认证。在移动存储介质内部和监控代理程序内部使用相同的对称密钥算法，采用挑战/应答式动态认证机制。移动存储介质如果通过认证，则可以进行绑定标记的匹配；否则，移动存储介质不能使用。

### 3.3 绑定标记概述

绑定标记用于将单位人员使用的移动存储介质和该人员使用的主机进行一一绑定。移动存储介质在与其绑定的主机上可读可写，在其他非绑定主机上为只读使用；单位外部的移动存储介质在单位内主机上为只读使用，确保了单位内主机上信息出口的唯一性，降低了敏感信息泄露的风险。移动存储介质通过绑定标记匹配后，可以进行等级标记的比较。

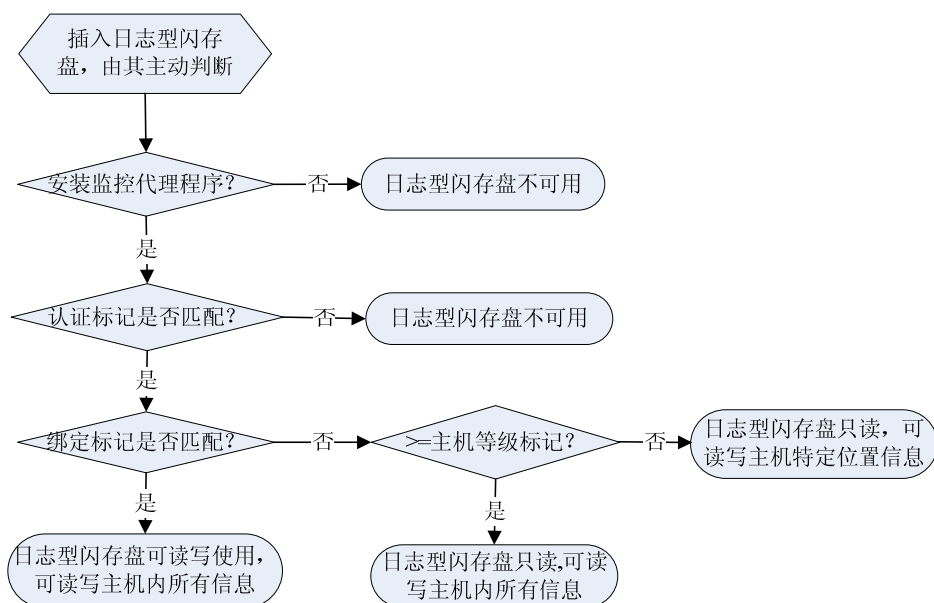


图2 日志型闪存盘的判断流程



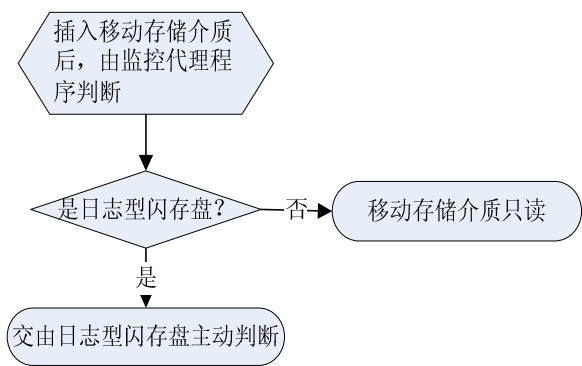


图3 监控代理程序的判断流程

4 基于日志型闪存盘实现安全管理机制

4.1 基于日志型闪存盘的安全管理系统相关功能概述

- 1) 日志型闪存盘自身具备加解密模块，采用军用对称密钥算法保证存储在其上信息的安全，具有主动控制代码，可实现对主机的主动认证功能，详细内容请参阅文献 10；
- 2) 基于日志型闪存盘研制安全管理系统，继续采用 C/S 架构；
- 3) 日志型闪存盘和监控代理程序使用相同的军用对称密钥算法，在此不作为重点阐述。

4.2 认证标记及其判断过程

- 1) 认证标记采用 Windows 自带的 timeGetTime( ) 函数、srand( ) 函数和 rand ( ) 函数生成 40 位长度的随机数，在管理主机上安装安全管理系统时由系统调用随机函数生成认证标记并存入管理系统。
- 2) 管理系统在对日志型闪存盘注册时，使用自定义的 SetAuthlabel ( ) 函数将上述产生的 40 位长度的认证标记写入日志型闪存盘内置的特殊存储器 EEPROM 中，该特殊存储器可存储包括加解密密钥、认证标记、绑定标记以及等级标记等关键参数，并具有防止非授权读取和破坏的功能。
- 3) 监控代理程序采用军用对称密钥算法，安装在客户端主机上时将该认证标记加密后存入客户端主机注册表，待需要使用时临时由监控代理程序解密出，使用自定义的 GetDiskSerialNumber ( )

函数获取客户端主机的主机硬盘 ID 作为加解密认证标记的密钥。

4) 动态认证过程：在日志型闪存盘插入单位内的客户端主机时，首先判断主机上是否安装有监控代理程序，没有安装的话则日志型闪存盘不可使用，已安装则进行如下认证步骤。

a) 日志型闪存盘使用内部随机函数生成一个随机数 P1 并保存起来，同时将 P1 发送给客户端主机监控代理程序，该随机数 P1 的生成方式与认证标记的生成方式相同；

b) 监控代理程序在收到随机数 P1 后，使用事先分发的认证标记作为加密密钥，采用对称密钥算法将 P1 进行加密得到密文 P1'，然后将 P1' 发送给日志型闪存盘；

c) 日志型闪存盘在收到 P1' 后，使用自身存储的认证标记作为解密密钥，采用和监控代理程序相同的对称密钥算法解密 P1' 得到 P1"，并与自身保存的 P1 相比较，若 P1"与 P1 相同则表示该日志型闪存盘在本单位注册过，通过认证，否则是外单位的客户端主机，日志型闪存盘不可使用；

d) 同时，如果是普通移动存储介质插入客户端主机，监控代理程序检测到非日志型闪存盘插入，则将这个普通移动存储介质设置为只读状态，防止其窃取客户端主机上敏感信息。

4.3 绑定标记及其判断过程

- 1) 绑定标记生成以及分发的步骤如下。
  - a) 管理系统在安装客户端主机监控代理程序时，要收集客户端主机信息，根据主机的硬盘 ID 以及网卡的 MAC 地址生成绑定标记，然后交由监控代理程序加密后存放在注册表中，同时将该绑定标记导入管理系统保存；
  - b) 管理系统在注册日志型闪存盘时，需要为该日志型闪存盘选择一台需要绑定的主机，然后将一一对应的绑定标记写入日志型闪存盘，实现时使用自定义 SetBindlabel ( ) 函数写入日志型闪存盘内置的特殊存储器 EEPROM 中。
  - c) 至此，日志型闪存盘与其对应的主机具有相同的绑定标记，否则绑定标记不相同。
- 2) 绑定标记的判断过程：与认证标记的判断过程一致，需要采用随机数进行加解密匹配判断，来决定日志型闪存盘与客户端主机是否一一绑定。

## 4.4 等级标记及其判断过程

1) 在管理系统注册日志型闪存盘时,由安全管理员根据其使用者的级别分为绝密、机密、秘密和无密四个安全级别,使用自定义 SetRanklabel() 函数对其等级标记进行设置;客户端主机也根据它的使用者级别,在安装监控代理程序时设置该主机的等级标记(如:将局以上干部使用的日志型闪存盘和主机设置为 3,处级为 2,科级为 1,科级以下为 0)。

2) 经过上述绑定标记的匹配,日志型闪存盘对于绑带主机为读写使用,对于非绑定主机设置为只读状态。对于非绑定主机需要进行日志型闪存盘等级标记与客户端主机等级标记的对比,日志型闪存盘的等级标记如果大于等于主机的等级标记,则可以读写主机上所有信息,否则只能读写主机上特定位置的信息(如:可将特定位置设置为“我的文

档”),其他文件夹都不可读取,可防止低安全级别的日志型闪存盘插入高安全级别的主机窃取敏感信息。

## 5 结束语

经过实际应用证明,基于日志型闪存盘实现的上述安全管理机制可以较好地完成对移动存储介质的认证、访问控制等安全管理功能,安全高效地防范敏感信息的泄漏问题,基本满足各单位使用移动存储介质进行安全信息交换的要求。下一步的重点工作是完善安全管理系统的日志审计功能,使其做到有案可查、有据可依。

## 参考文献

- [1] 黄淑宽,林柏钢.常用的口令认证机制及其安全性分析.网络安全技术与应用,2005.6:29-31.
- [2] 李雪.标识认证打开信息安全新天地.信息安全与通信保密,2006.9:9-11.
- [3] 石文昌,孙玉芳,梁洪亮.经典 BLP 安全公理的一种适应性标记实施方法及其正确性.计算机研究与发展,2001.11,38(11):1366-1372.
- [4] 张爱华,林园.一种基于安全标签的访问控制模型的设计和实现.计算机应用研究,2007,1:183-185.
- [5] 梁洪亮,孙玉芳,赵庆松等.一个安全标记公共框架的设计与实现.软件学报,2003,14(3):547-552.
- [6] 席丽萍.笔记本电脑和移动存储介质的管理方略.创新科技,2006.10:42-43.
- [7] 刘东辉,严祺.公安机关计算机信息泄密的主要渠道及防范措施.吉林公安高等专科学校学报,2005,5:47-50.
- [8] 何祥勇.浅谈移动办公的信息安全.华南金融电脑,2006.10,10:12-14.
- [9] 张世永.网络安全原理与应用.北京:科学出版社,2003.5.
- [10] 刘宝生,日志型闪存盘的设计与实现,解放军理工大学硕士学位论文,2006.2.

## 作者联系方式

通信地址:北京市丰台区大成路13号A00

邮政编码:100039

联系电话:13439934550 010-66820269-872



# 第三代移动通信系统安全体系结构研究

郭智恩 谢永强

**摘 要：**论文从分析移动通信系统面临的安全威胁入手，介绍了第三代移动通信系统的安全结构，讨论了其采用的安全新技术，包括用户认证、用户身份保密、以及通信过程中数据完整性保护和数据加密方法，最后指出 3G 系统的安全性缺陷和军队 3G 系统的安全性建议。

**关键词：**第三代移动通信；3G；系统安全；认证与密钥协商

## 1 概述

随着移动通信技术的不断发展，第三代移动通信系统（The 3rd Generation Mobile Communication System，以下简称 3G 系统），技术已经日趋成熟。3G 系统（第三代移动通信系统）是一个在全球范围内覆盖与使用的通信网络系统，所提供的业务除了传统的语音业务外，还包括多媒体业务、数据业务，以及电子商务、电子贸易和互联网服务的多种信息业务。因此在 3G 系统中，安全性要求尤为重要。3G 系统是在 2G 系统的基础上发展起来的，其安全结构是在支持 2G 系统安全特征的基础上，针对新业务特点以及进一步提高通信安全性设计的，提供了更加完善的安全保障体系。

## 2 移动通信中的安全威胁

无线信道的开放性使移动通信网络面临着更多的安全威胁，如窃听和假冒。因此，移动通信中的安全性受到越来越多的关注。移动通信中的安全性主要包含三个方面。机密性：非授权获取通信内容；完整性：非授权修改敏感技术；认证性：非授权使用网络提供的服务。

然而不是提供了一定的安全机制就可以一劳永逸地享受移动通信网络安全。安全威胁在变，安全机制需要与时俱进。信息安全领域中永远不存在坚不可摧的安全防御体系，新的攻击方式总是不断地催生新的防御手段，而新的防御手段又激发更新的攻击方式。移动通信系统所面临的主要威胁如下。

- 对敏感数据的非法获取，对系统信息的保密性进行攻击，其中主要包括：

- 1) 侦听：攻击者对通信链路进行非法窃听，获取消息；
- 2) 伪装：攻击者伪装合法身份，诱使用户或网络相信其身份合法，从而窃取系统信息；
- 3) 流量分析：攻击者对链路中消息的时间、速率、源及目的地等信息进行分析，从而判断用户位置或了解重要的商业交易是否正在进行；
- 4) 浏览：攻击者对敏感信息的存储位置进行搜索；
- 5) 泄露：攻击者利用合法接入进程获取敏感信息；
- 6) 试探：攻击者通过向系统发送信号来观察系统反应。
  - 对敏感数据的非法操作，对消息的完全性进行攻击，主要包括：对消息的篡改、插入、重放或删除。
  - 对网络服务的干扰或滥用，从而导致系统拒绝服务或导致系统服务质量的降低，主要包括：
    - 1) 干扰：攻击者通过阻塞用户业务、信令或控制数据使合法用户无法使用网络资源；
    - 2) 资源耗尽：用户或服务网络利用其特权非法获取非授权信息；
    - 3) 服务滥用：攻击者通过滥用某些系统服务，从而获取好处，或者导致系统崩溃
      - 否认，主要指用户或网络否认曾经发生的动作。
      - 对服务的非法访问，主要包括：
        - 1) 攻击者伪造成网络和用户实体，对系统服务进行非法访问；
        - 2) 用户或网络通过滥用访问权利非法获取未授权服务。

### 3 3G系统安全体系结构

3G 系统安全结构中共定义了 5 组安全特性（如图 1），每一组安全特性针对特定的威胁，并完成特定的安全目标。

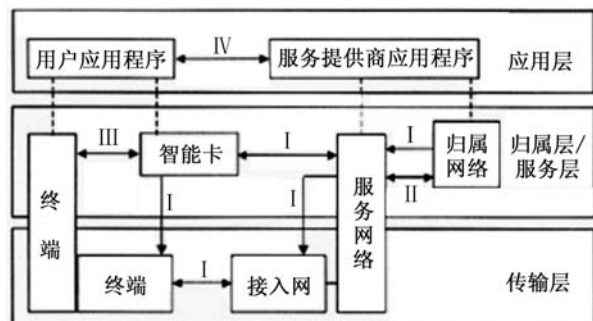


图1 3G系统安全体系结构

① 网络接入安全（I）：定义了为用户提供安全接入 3G 服务的安全特性，特别强调防止无线接入链路的攻击；② 网络域安全（II）：定义了在营运商结点间安全传输数据的安全特性，并保护对有线网络的攻击；③ 用户域安全（III）：定义了安全接入移动站的安全特性；④ 应用程序域安全（IV）：定义了用户应用程序与营运商应用程序安全交换数据的安全特性；⑤ 安全的可见度与可配置性（V）：定义了用户能够得知操作中是否安全，以及对安全程度自行配置的安全特性。

### 4 3G系统的安全新技术

3G 移动通信系统中的安全技术是在 2G 的安全基础上建立起来的，它克服了 2G 系统中的安全问题，也增加了新的安全功能，下面从用户身份保密、认证以及数据传输的保密性与完整性等几个方面对 3G 系统中主要的安全防范策略加以介绍。

#### 4.1 认证

3G 系统的实体间认证过程比原有 2G 系统认证功能增强很多，且增加了新功能，具体有以下 3 方面。

- 1) 3G 系统完成了网络和用户之间的双向认证；
- 2) 3G 系统增加了数据完整性这一安全特性，以防止篡改信息这样的主动攻击；

3) 在认证令牌 AUTN 中包括了序列号 SQN，保证认证过程的最新性，防止重新攻击，并且 SQN 的有效范围受到限制。

3G 中的认证使用了 5 参数的认证向量 AV（RAND、XRES、CK、IK、AUTN），执行 AKA（Authentication and Key Agreement）认证和密钥协商协议，如图 1 所示，HE/HLR 表示用户归属区的用户归属寄存器；AV 表示认证向量；AUTN 表示认证令牌；RES 和 XRES 分别表示用户域的应答信息和服务网的应答信息；RAND 表示生成的随机数；CK 和 IK 分别表示数据保密密钥和数据完整性密钥。

AKA 协议可分为 2 部分，第一部分是用户归属域 HE 到服务网 SN 认证向量的发送过程，SN（由 VLR/SGSN 实体执行）向 HE（由 HLR 实体执行）申请认证向量，HE 生成一组认证向量 AV（1, ..., n）发送给 SN，SN 存储收到的认证向量；第二部分是认证和密钥建立的过程，SN 从收到的一组认证向量中选择一个 AV（i），将 AV（i）中的 RAND（i）和 AUTN（i）发送给用户的 USIM 进行认证。用户收到 RAND 和 AUTN 后计算出消息认证码 XMAC，并与 AUTN 中包含的 MAC 相比较，如果二者不同，USIM 将向 VLR/SGSN 发送拒绝认证消息。如果二者相同，USIM 计算应答信息 XRES（i），发送给 SN。SN 在收到应答信息后，比较 XRES（i）和 RES（i）的值。如果相等则通过认证，否则不建立连接。最后在认证通过的基础上，MS/USIM 根据 RAND（i）和它在入网时的共享密钥 K（i）来计算数据保密密钥 CK（i）和数据完整性密钥 IK（i）。SN 根据发送的 AV 选择对应的 CK 和 IK。

#### 4.2 用户身份保密

3G 系统中的用户身份保密有三个方面的含义：

- 1) 在无线链路上窃听用户身份 IMSI 是不可能的；
- 2) 确保不能够通过窃听无线链路来获取当前用户的位置；
- 3) 窃听者不能够在无线链路上获知用户正在使用的不同的业务。

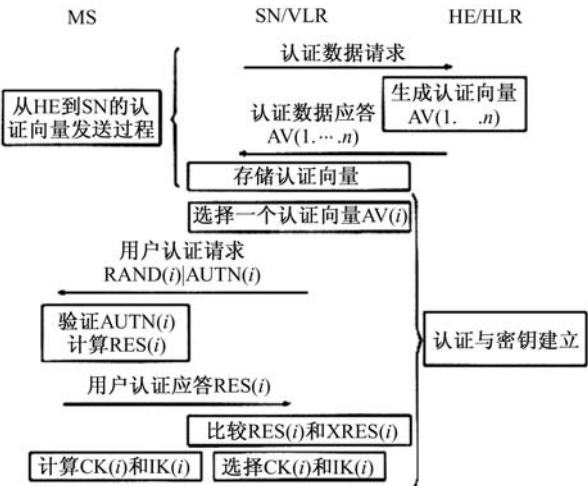


图2 3G 的认证与密钥协商 (AKA) 协议

为了达到上述要求, 3G 系统使用了 2 种机制来识别用户身份:

- 1) 使用临时身份 TMSI;
- 2) 使用加密的永久身份 IMSI。

而且要求在通信中不能长期使用同一个身份。另外为了达到这些要求, 那些可能会泄露用户身份的信令信息以及用户数据也应该在接入链路上进行加密传送。在 3G 中为了保持与第二代系统兼容, 也允许使用非加密的 IMSI, 尽管这种方法是不安全的。

在使用临时身份机制中, 网络给每个移动用户分配了一个临时身份 TMSI。该临时身份与 IMUI 由网络临时相关联, 用于当移动用户发出位置更新请求、服务请求、脱离网络请求, 或连接再建立请求时, 在无线链路上识别用户身份。当系统不能通过 TMUI 识别用户身份时, 3G 系统可以使用 IMSI 来识别用户, 如图 3 所示。

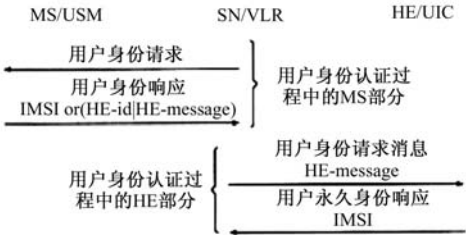


图3 永久用户身份识别机制

该机制由拜访的 SN/VLR 发起向用户请求 IMSI。由于使用 IMSI 的明文传送, 可能导致 IMSI 被窃听。在 3G 中使用加密的用户身份。在收到 SN/VLR 的身份请求后, MS/USIM 把 IMSI 加密后

嵌入 HE-message 中, 并且用 HE-id 来向 SN/VLR 指明可以解密该 HE-message 的 HE/UIC 的地址。SN/VLR 收到 HE-message 后, 根据 HE-id 再把该消息传送到相应的 HE/UIC, HE/UIC 解密后把用户的 IMSI 传递给 SN/VLR。在收到用户的 IMSI 后, 就可以启动 TMSI 分配过程, 此后将使用 TMSI 来识别移动用户身份。这种增强型身份加密机制把原来由无线接入部分传送明文 IMSI 变成在网络内传送明文 IMSI, 在一定程度上加强了用户身份的机密性。

4.3 数据保密

在 3G 系统中, 网络接入部分的数据保密主要提供 4 个安全特性: 加密算法协商、加密密钥协商、用户数据加密和信令数据加密。其中加密密钥协商在 AKA 中完成。加密算法协商由用户与服务网间的安全模式协商机制完成。在无线接入链路上仍然采用分组密码流对原始数据加密, 采用了 f8 算法, 如图 3 所示。它有 5 个输入: ① COUNT 是密钥序列号; ② BEARER 是链路身份指示; ③ DIRECTION 是上下行链路指示; ④ LENGTH 是密码流长度指示; ⑤ CK 是长度位 128bit 的加密密钥。

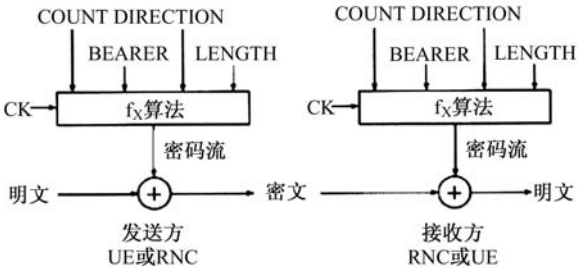


图4 3G 数据加密

与 2G 相比, 3G 不仅加长了密钥长度, 而且引入了加密算法协商机制。当移动终端 ME 需要与服务网 SN 建立连接时, USIM 告诉服务网它支持哪些加密算法。服务网根据下列规则做出以下判断。另外在 2G 中的加密是基于基站, 消息在网络内是用明文传送, 这显然是很不安全的。3G 加强了消息在网络内的传送安全, 采用了以交换设备为核心的安全机制, 加密链路延伸到交换设备, 并提供基于端到端的全网范围内加密。

## 4.4 数据完整

在移动通信中, MS 和网络间的大多数信令信息是非常敏感的, 需要得到完整性保护。在 3G 中采用了消息认证来保护用户和网络间的信令消息没有被篡改。数据完整性保护方法如图 4 所示。

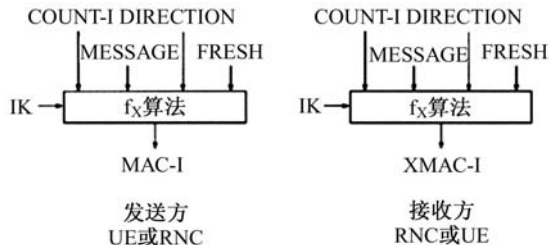


图5 数据完整性验证

发送方把要传送的数据用完整性密钥 IK 经过  $f_K$  算法产生消息认证码 MAC, 将其附加在发出的消息后面。在接收方把收到的消息用同样的方法计算得到 XMAC。接收方把收到的 MAC 与 XMAC 相比较, 如二者相同就说明收到的消息是完整的。

3G 数据完整性主要提供 3 个安全特性: 完整性算法 (UIA) 协商、完整性密钥协商、数据和信令的完整性。其中完整性密钥协商在 AKA 中完成; 完整性算法协商由用户与服务网间的安全模式协商机制完成, 完整性算法协商与加密算法协商过程相似, 在这里就不详细叙述了。3G 系统预留了 16 种 UIA 的可选范围, 目前只用到一种算法 Kasumi。

## 5 安全缺陷及完善建议

虽然 3G 的安全性能在密钥长度、算法选定、鉴别机制和数据完整性检验等方面, 远远优于前两代移动通信技术。但 3G 仍然存在下列安全缺陷, 虽然 3G 在密钥长度、算法的完善性、认证机制和数据完整性检验等方面提供的安全性能远远优于 2G, 但它仍然存在一些安全缺陷: ① 3GPP 允许参考文献 (略)

### 作者联系方式

通信地址: 北京丰台区大成路 13 号院 A00

邮政编码: 100039

联系电话: 010-66820269—812 13366330296

将比较弱的加密算法标准化以便于出口, 使很多网络不能提供开展电子商务和电子银行所必需的加密级别, 用户在网络漫游时不得不使用第三方的方案和服务来解决应用层和会话层的安全; ② 没有建立公钥密码体制, 难以实现用户数字签名, 密码学的最新成果也未能得到应用; ③ 终端存储能力和处理能力的增强在有利于更多数据业务和电子商务的开展的同时, 也利于病毒的传播。正是由于这些缺陷的存在, 新的攻击方式不断涌现出来, 使 3G 网络面临着新的挑战。

但随着 3G 技术日渐成熟, 3G 取代 2G 投入军队使用将成为必然, 军队 3G 系统的安全将可以从以下几个方面加以发展和完善。

1) 建立适合军队移动通信系统的安全体系结构模型: 如, 在网络安全体系结构模型中, 应能体现网络的安全需求分析、实现的安全目标等。

2) 由私钥密码体制向混合密码体制的转变: 军队移动通信系统中, 针对不同的安全特征与服务, 采用私钥密码体制和公钥密码体制混合的体制, 同时加快建设无线公钥基础设施 (WPKI), 建设中国移动的以 CA (认证中心) 为核心的安全认证体系。

3) 新密码技术的广泛应用: 随着密码学的发展以及移动终端处理能力的提高, 新的密码技术如量子密码技术、椭圆曲线密码技术、生物识别技术等, 在军队移动通信系统中获得广泛应用, 加密算法和认证算法自身的抗攻击能力更强健, 从而保证传输信息的机密性、完整性、可用性、可控性和不可否认性。

4) 移动通信网络的安全措施更加体现面向用户的理念: 用户能自己选择所要的保密级别, 安全参数既可由网络默认, 也可由用户个性化设定。

# 可信军用通信网络基础技术

刘建军 顾晓鸣

**摘 要:** 当前,我军通信网络可信性存在严重欠缺,越来越制约各类应用的发展。本文分析了军用通信网络面临的安全挑战和国内外网络安全领域的发展现状,提出了可信军用通信网络基础技术及今后的研究方向。

**关键词:** 可信; 网络安全; 通信网络

## 1 概述

经过多年的建设和不断发展,我军各类军用通信网络已经渗透到军事应用的各个领域,成为军队信息化的基础设施。由于军用通信网络越来越多地采用民用互联网技术实现,其体系结构存在难以克服的安全及管理等方面的问题,军用通信网络天生的泛在性和动态特性更导致其可信性存在严重欠缺,越来越制约各类应用的发展。开展可信军用通信网络基础技术的研究是实现高度可信的信息资源共享和协作,为各类军事应用系统提供可信保障的关键,成为当前我们必须密切关注和积极从事的重要课题。

## 2 军用通信网络面临严峻的安全挑战

从最初美军将计算机网络应用于军事通信开始,军用通信网络是应用于非商业、友好型的环境,其基本假定是业务流是可信任的,主要侧重于网络的简单性、开放性和高效性,对恶意攻击几乎不设防,安全体系存在先天不足。另外,网络设计者认为链路加密对网络安全有足够的保障,网络放弃了承担安全性的责任。随着军队信息化水平越来越高,军用通信网络应用范围越来越广,网络安全问题也日益突出,网络上威胁频次、影响、规模和代价明显增加,通过网络的失窃密事件屡屡发生,军事指挥人员普遍对网络安全感到担忧,严重影响军事通信网络的应用。

另一方面,我军通信网络大量采用民用的通用技术和国际标准,这些技术和标准主要是以商业应用为目标,难以适应我军对通信网络安全有严格要

求的军事需求。完全依靠民用研究,难以满足军事应用的需求。此外,受我国电子信息产业整体实力的制约,我军通信网络采用的网络设备、微处理器、操作系统和基础应用软件很多依赖进口,或者其中的关键技术和芯片使用国外产品,在信息战已成为重要作战样式的今天,这就难免被嵌入病毒、后门和窃密装置,成为我军通信网络系统严重的安全隐患。

## 3 可信通信网络概念

在 X.509 标准中对可信的定义是:“如果实体甲认为乙的行为符合甲的期望,那么可以说乙是可信的。”而对于可信通信网络,目前还没有统一的定义,但是专家们逐渐取得了新的共识,认为可信性比安全性具有更广泛的技术内涵,可信是信息保障概念的延续。可信通信网络中实体的行为是可知的、可控的,行为的结果是可预期的。可信通信网络包括三个基本属性:安全性、可管控性和可生存性。

可信通信网络的安全性除了传统意义上的安全性(即保密性、完整性、可用性)之外,还应该具有真实性、可审计性、私密性等特性。可管控性包括对网络的可管性和可控性两个方面。即网络必须提供更方便、灵活的管理手段,对违反网络安全政策的行为具有控制能力。可生存性是指在遭受攻击、故障或意外事故时,依然提供网络基本服务的能力,以及在一定时间内修复受损服务的能力。

## 4 国内外研究现状

近年来,世界上许多国家认识到网络信息安全关系国家战略安全,把网络信息安全放在优先发展的位置,竞相开展相关的研究。2003年至2006年美国先后发布了《保护赛博空间的国家战略》《赛博安全(Cyber Security):优先考虑的危机》和《联邦政府赛博安全与信息保障研发计划》,这三份文件在全面分析美国信息基础设施和关键基础设施面临威胁的基础上,提出了赛博安全的新思维、新战略和新动向。在此思想的指引下,美国开展了一系列具有影响力的研究项目,如NSF(美国自然科学基金会)于2005年8月公布的全球网络创新环境(GENI, Global Environment for Network Innovations),是一项由政府主导的重大网络创新行动,不仅是技术创新,而且体系结构也要创新。NeTS-FIND(The Network Technology and Systems Program-- Future Internet Design)是美国科学基金会NSF于2004年提出的一个新的长期计划,旨在推动新的下一代网络基础设施体系的尽早出现。FIND资助在网络体系结构、原则和设计等多领域的研究。另外,其他的国家也相当重视可信网络的研究,如,俄罗斯把信息安全作为重建大国地位的关键;西欧各国和日本、韩国、印度、新加坡等也都从国家发展战略、安全战略和军事战略的高度奋起直追,加强了安全战略的制定,并围绕创建网络安全、打击网络犯罪、保护数据和资源等课题展开探索。

在国内,也非常重视下一代可信网络基础理论的研究,启动了包括国家973、国家自然科学基金、863、发改委CNGI等项目。国家自然科学基金委2001年度启动了重大研究计划《网络与信息安全》,重点研究下一代互联网的体系结构,控制及网络行为。国家973项目组于2003年度资助了重大研究计划《新一代互联网体系结构理论研究》,重点就是重新设计规划互联网的体系结构。2005年度国家863项目批准了北京交通大学等关于《一体化网络服务新技术研究》的创新预研课题,重点研究新一代一体化网络的业务控制和恢复技术。北京交通大学在国家973项目“一体化可信网络与普适服务体系基础研究”中,提出了两层新一代网络体系模型,实现对普适服务的支持。

## 5 可信军用通信网络基础技术

我军通信网络是一个多种技术体制共存、多种网系的复杂大系统。可信军用通信网络的构建是一个复杂的系统工程,不可能依靠单一技术来实现,必须是多种基础技术综合作用,才能达到整体可信的效果。目前来看,我们认为可信军用通信网络基础技术至少包括以下几个重要的方面。

- 可信军用通信网络体系架构;
- 可信军用通信网络基础协议;
- 信源定位技术;
- 可信评测和管理方法;
- 网络可生存性技术。

### 5.1 可信军用通信网络体系架构

当前大部分军用计算机网络安全系统主要是由防火墙、入侵检测和病毒防范等组成,采取“堵漏洞、筑高墙、防外攻”等修补式安全架构,具有严重的滞后性。对于军用通信网络这样的复杂多层次基础设施来说,安全威胁和相应的控制机制都必须从系统的视角来认识,其可信性所需要的不仅仅是其组成部分的安全性;还需要研究如何使大型且复杂的系统从整体上具有可信性。最终,基础研究应解决包括硬件、操作系统、网络传送、控制和应用各个层面在内的整体可信的全新网络体系架构。

可信军用通信网络体系结构设计目标是彻底摆脱当前网络体系结构的束缚,依据未来的军用通信网络需求和当前的设计条件,重新确定设计目标 and 设计原则,指导体系结构的设计和协议、技术的选择,形成整体可信的军用通信网络架构。主要研究方向包括:

- 明确我军通信网络应用需求,提出总体设计目标和设计原则。
- 设计满足安全可信要求的新型寻址、命名、标识等体系结构,设计新的路由转发及网络管理机制。
- 研究可信军用通信网络体系结构定义、验证、评估与测试的方法。

### 5.2 可信军用通信网络基础协议

最初的军用通信网络遵循与传统互联网同样的设计理念,网络协议以“在充分可信赖环境下”来

设计,然而,对于军用通信网络而言,其工作于一种可能受到攻击的环境,安全性受到严重威胁,基本标准都必须加入安全考虑,从基本传输机理上重新制定基础协议的安全版本。因此,可信军用通信网络基础协议的目标是通过重新设计网络协议,为网络实体间在信息传送过程中的发信、转发、接受等提供可信证据,解决网络层面的可信信息传送问题。主要研究方向包括:

- 深入研究当前主要的网络传送技术和网络传送机理,如标签、虚电路、数据流路径、认证和保密能力等。
- 研究能够提供信息传送可信证据的技术方案,明确可信军用通信网络协议功能需求。
- 根据功能需求,进行可信网络军用通信网络基础协议设计。

### 5.3 信源定位技术

军用通信网络大量采用 TCP/ IP 基础技术,运营商设备、协议乃至网络拓扑对终端用户均是开放的,通过终端与运营商网络交换非法的恶意路由信息,即可对运营商网络的路由器、接入服务器等设备三层以上设备实施攻击。另外,网络终端高度智能化使终端用户发动攻击变得容易,又增加了识别与防范各类花样繁多的安全攻击的难度。由此可见,安全攻击多半在终端发起,军用通信网络最大的安全漏洞是缺少对源地址的确认,非法用户可以容易侵入军用通信网络,可以通过网络攻击其他计算机,而且事后又未留下地址,或者地址不可信(可以伪造)。这就是军用通信网络失窃密的主要原因,也是网络对抗条件下网络安全的主要威胁之一。

因此,如果能够实时或迅速发现攻击者真实的网络地址,并进一步确认物理地址,就可以采取安全措施,阻断非法用户的接入或其恶意行为的实现,信源定位的能力是军用通信网络安全技术的前沿课题。信源定位技术主要是针对网络出现的异常流量,在记录其真实源地址的情况下,通过对其源头的溯源,快速找到进入网络的源地址,定位攻击点或问题点。主要研究方向包括:源地址地址分配策略、溯源和反向追踪方法、源路径隔离技术。

### 5.4 可信评测和管理方法

在当前开展的可信通信网络研究中,对可信评测和管理方法的研究是相对薄弱的,多数情况下仍沿用网络安全的评测标准和管理方法,对可信评测和管理的重要性认识得并不充分。人们初步认识到,对于网络的可信程度的评价应该客观公正,但评价本身属于主观行为,难以确定客观的评价标准,另一个难点是各类军事应用需求不同,如何为“可信”分等级。上文提到的 GENI 计划一个重要的任务是建立能够容纳多种体系架构的试验床,通过系统的进化和择优,得到最佳的网络体系架构,是一种实践检验的评测方法。从管理的角度看,可信通信网络需要科学、可信的管理方法,需要对所有计算机网络应用体系中各个方面的可信技术和产品进行统一的管理和协调,进而从整体上提高整个计算机网络的可信等级的能力。今后我们的主要研究方向是:如何建立一个综合的评测指标体系;如何在试验床中保证各种体系架构的兼容;如何实现对网络中资源动态可信的管理。

### 5.5 网络可生存性研究

网络生存性是指网络系统在遭受攻击、出现故障、或发生意外事故时,依然能够及时完成任务的能力。为了增强网络的可生存性,传统的网络采取了备份、负载均衡、硬件冗余等安全措施。随着对网络基本原理认识的不断深入,人们发现需要发展新的理论提高网络的可生存能力。可生存能力意味着网络可以被入侵,可以部分组件受损,乃至某些部件并不完全可靠,但只要网络能在结构上合理配置资源,能在攻击下资源重组,就可以实现网络的自优化、自维护、自调节等自我保护能力。主要研究方向包括:复杂系统理论及网络动力学行为理论,基于自适应网络路由算法及网络资源的快速动态配置策略,通信网络自组织和自愈重构关键技术等。

## 6 发展可信军用通信网络的必要性

军用通信网络保障能力是军队信息化发展的重要基础,是军队现代化建设水平的重要指标。在信息战和网络中心战成为新的作战样式形势下,军事通信网络领域的对抗将是二十一世纪军事对抗焦

点, 军用通信网络比起民用网络, 在安全性、可控性和可生存性方面都有更高的要求, 网络的可信问题更加突出, 也更加迫切。我军通信网络发展水平与发达国家相比, 还有不小的差距, 完全依靠国外技术, 永远无法缩小与外军水平的差距。完全依靠国内市场导向的技术发展, 也难以与外军发展相

竞争。因此, 我们必须从国家战略高度认识网络可信问题, 加大我军在可信军用通信网络上的科研投入, 与国家基础研究投入及业界商业投入相结合, 促进可信军用通信网络研究的快速发展, 对于加快我军信息化建设具有重要意义, 也是赶超外军先进水平的必要举措。

### 参考文献

- [1] 中国信息安全产业发展白皮书(2005—2010), 中国信息产业商会信息安全产业分会, 2005
- [2] The National Strategy to Secure Cyberspace February, 2003
- [3] GENI Design Document, <http://www.geni.net/>

### 作者联系方式

通信地址: 北京市丰台区大成路13号 W00

邮政编码: 100039

联系电话: 010-66820390



# 电子军务安全与混沌加密

刘益 郝明

**摘 要:** 介绍了电子军务的安全隐患及现行安全策略, 提出混沌加密的三种方法并对其进行了分析比较。

**关键词:** 电子军务; 安全隐患; 安全策略; 混沌加密

## 1 混沌理论介绍

混沌(chaos)是自然界及人类社会中一种普遍现象, 它是在一个确定系统中出现的一种貌似不规则的、内在的随机性运动, 展示了事物的复杂性。混沌实际上并不“混”, 既非纯粹的“无序”, 又非纯粹的“有序”, 而是两者的统一, 即有序与无序的统一, 确定性与随机性的统一, 具有内在的规律性和普适性。

混沌系统内包含无数的不稳定周期轨道和非周期轨道, 它们极其稠密地集中在混沌奇异因子中; 混沌系统在满足某种条件下, 可以构成一个同步系统, 同时它对初始条件极为敏感, 两个几乎相同的混沌系统, 其初态稍异就会迅速变成完全不同的状态; 混沌系统的行为是许多有序行为的集合, 而每个有序分量在正常条件下, 都不起主导作用。混沌系统提供了良好的随机、相关、复杂的拟随机序列<sup>[1]</sup>。正因为混沌系统有这些特点, 用其对信息进行加密是当前研究的主要热点。电子军务要求高度安全性, 利用混沌系统对信息加密可提高保密性, 本文分析了三种混沌加密算法, 并对其进行了分析比较。

## 2 电子军务现状分析

### 2.1 电子军务安全隐患

电子军务是军事信息网应用发展的必然趋势, 在现行的业务交流中发挥着越来越重要的作用, 给部队工作带来了便利。同时, 电子军务运行在军队网络上, 在军队要求高度保密的条件下, 网络安全是实现电子军务的关键。但由于网络环境相对比较开放, 运行在网络上的设备和软件多种多样, 存在

一些安全隐患, 攻击者利用这些漏洞对网络进行攻击, 下面介绍几种主要的攻击手段。

1) 信息在传输过程中被截取。攻击者可通过多种方式对网络中传输信息进行监听并截取。可通过在传输介质有电磁波辐射范围内安装接收装置, 截获传输的机密文件信息。或是通过网络使用诱探工具捕捉数据包获得情报。

2) 假冒身份。攻击者假冒身份登录, 冒充领导调阅机密文件, 散布虚假信息, 套取、修改密钥和使用权限等。或冒充网络控制程序, 非法获取信息等。

3) 信息被篡改。对系统完整性进行攻击, 修改文件中的数据, 使接受用户阅读虚假信息。或是替换某一段程序, 使其不能执行某项功能。

4) 计算机木马。在计算机中植入木马, 在计算机运行某些程序时, 木马自动开启, 通过网络窃取机密文件。

### 2.2 电子军务安全策略

电子军务要求信息高度保密性、完整性、真实性, 而现在攻击者手法多样, 对网络安全环境提出了严峻的考验。目前保障电子军务信息安全的策略有以下几个方面。

1) 防火墙。防火墙是目前使用最广泛、最普遍的网络安全技术, 用来分隔可信网络和不可信网络的设备。主要运用了三种检测方法, 分别是分组过滤和无状态过滤; 状态过滤和深度分组检测。可以通过监视、限制、更改数据流, 对外屏蔽内部网络拓扑结构、对外屏蔽危险站点, 防范非法访问, 具有比较强的控制功能。

2) 入侵检测。它是检测任何企图损害系统保密性、完整性或可用性的一种网络安全技术。当发现某个数据分组或一系列数据分组表现出可疑的违

反安全策略的行为时,触发相应的事件警告。可根据监测对象划分为三类:基于主机的入侵检测系统、基于网络入侵的检测系统和混合型入侵检测系统。

3) 加密与解密。现在密码技术比较成熟,应用比较广泛,传输机密信息、身份验证都要使用密码技术。主要有对称密钥算法和非对称密钥算法。对称密钥算法(Symmetric Key Algorithm)使用相同的密钥进行加密和解密,双方在进行安全通信之前必须共享密钥。而非对称密钥算法(Asymmetric Key Algorithm)适用一对不同的密钥来加密和解密。

4) 其他安全策略。在应用上述安全防范手段的同时,还有其他安全防范措施,如访问控制,限制访问级别与权限;信息备份与恢复,防止信息丢失或失真;防写措施,将信息设置为“只读”,用户只能读取信息,不能修改。

### 3 混沌加密

现在研究人员已经认识到了传统密码学的不足,混沌作为一种非线性现象,可以为密码学提供新思路,为保密通信提供更好的手段,用于电子军务可提高其安全性能。混沌密码学大致可分为两个大的研究方向,一个是利用混沌系统构造流密码,典型的由基于搜索机制的混沌密码和基于散列的混沌密码;另一个是以调制技术为核心的混沌保密通信。

#### 3.1 基于搜索机制的混沌密码

E.Alvarez<sup>[2]</sup>和 M.S.Baptista<sup>[3]</sup>提出了两类基于搜索机制的混沌加密。这两种算法都有其特殊性,都不属于流密码或者分组密码的范畴。其中 M.S.Baptista 提出设计方法引起了人们的关注。

Baptista 把数字区间划分成 256 个间隔区间(用  $\varepsilon$  表示),每一个间隔区间对应一个字母或符号。然后选择第一个明文作为混沌系统的初始值,于是混沌系统进行迭代,直到迭代值进入第二个明文所对应的间隔区间,此时把混沌系统的迭代次数作为该明文的密文。其形式化描述如下<sup>[4]</sup>。

给定一个一维混沌映射  $F: X \rightarrow X$ , 将一个子区间  $[x_{\min}, x_{\max}] \subseteq X$  划分为  $S$  个  $\varepsilon$  区间

$X_1 \sim X_s: X_i = [x_{\min} + (i-1)\varepsilon, x_{\min} + i\varepsilon]$ , 这里  $\varepsilon = (x_{\max} - x_{\min})/S$ , 假设明文消息由  $S$  个不同的字符  $\alpha_1, \alpha_2, L, \alpha_s$  组成, 使用一个双射:

$$f_s: X_i = \{X_1, X_2, L, X_s\} \rightarrow A = \{\alpha_1, \alpha_2, L, \alpha_s\} \quad (1)$$

将不同的  $\varepsilon$  区间和不同的字符关联起来。定义一个新的函数  $f'_s: X \rightarrow A$ ; 如果  $x \in X_i$ , 则  $f'_s(x) = f_s(X_i)$ 。

给定一个明文消息  $M = \{m_1, m_2, L, m_i, L\} (m_i \in A)$ , 其混沌密码算法描述如下。

混沌系统: Logistic 映射  $F(x) = \mu x(1-x)$ 。

密钥: Logistic 映射的初始条件  $x_0$  以及控制参数  $\mu$ 。

加密过程:

第一个明文字符  $m_1$ : 从  $x_0$  开始迭代混沌系统寻找一个满足  $f'_s(x) = m_1$  的混沌状态  $x$ , 记录迭代次数  $C_1$  作为第一个密文消息单元, 并计算  $x_0^{(1)} = F^{C_1}(x_0)$ ;

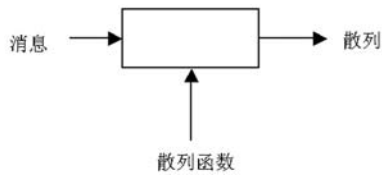
第  $i$  个密文单元密文  $x_0^{(i-1)} = F^{C_1+C_2+L+C_{i-1}}(x_0)$  开始迭代混沌系统寻找一个满足  $f'_s(x) = m_i$  的混沌状态  $x$ , 记录迭代次数  $C_i$  作为第  $i$  个密文消息单元, 并计算  $x_0^{(i)} = F^{C_i}(x_0^{(i-1)})$ ;

解密过程: 对每个密文单元  $C_i$ , 从上一次混沌状态  $x_0^{(i-1)} = F^{C_1+C_2+L+C_{i-1}}(x_0)$  开始迭代混沌系统  $C_i$  次, 使用  $x_0^{(i)} = F^{C_i}(x_0^{(i-1)})$  和关联映射  $f_s$  导出明文字符  $m_i$ 。

#### 3.2 基于单向散列的混沌加密

散列是一种保证数据完整性的机制, 它基于单向数学函数, 其特点是在一个方向上计算很容易, 但在相反方向计算原始值却很困难则很困难。打碎玻璃就是一个很好的例子, 玻璃杯很容易被打成碎片, 但是要将这些小碎片拼合成一个完整的杯子则几乎是不可能的。目前利用散列进行加密的算法有 MD5 和 SHA-1 两种。

文献[5]给出了基于混沌散列加密的设计思路。同样在这里给定一个一维的映射区间  $[x_{\min}, x_{\max}]$ , 将其分为  $N$  个区间, 并给每个区间编号, 每个区间对应一个 ASCII 字符。



混沌系统: Logistic 映射  $F(x) = \mu x(1 - x)$ 。

密钥: Logistic 映射的初始条件  $x_0$  以及控制参数  $\mu$ 。

Hash 函数:  $H_i = (H_{i-1}(x_{\max} - x_{\min}) * N / (x_{\max} - x)) \bmod N$  加密过程: 将明文第一个字符进入 Logistic 方程进行迭代, 直到轨道进入明文字符对应的区间。加密第  $i$  个字符时, 利用 Hash 算法对表进行更新。第  $H_i$  栏与  $H_{i-1}$  栏进行交换。不同明文对应不同查询表。

解密过程: 使用密钥和初始查询表进行相应次数迭代, 求出  $X$  实际值找到对应的明文, 解密第一个字符, 然后 Hash 算法对查询表进行更新操作, 在新查询表中对后续密文找到相应的明文。

3.3 基于调制的混沌加密

混沌调制又称宽谱发射, 是 Halle<sup>[6]</sup>等人提出解决秘密通信中复杂问题的技术之一。基本思想是将一个信息注入到发射机, 由此改变了原混沌系统的动态特性, 因此信号被调制, 混沌调制信号可以把信号谱的整个范围都用来隐藏信息, 而且增加了对参数变化的敏感性, 从而增强了保密性。

其调制方法是对需保密信号  $s(t)$ , 引入决定性的伪随机噪声信号  $x(t)$  相调制形成隐蔽的合成信号  $W(t)$ , 主要有以下三种:

- 1) 相乘  $W(t) = x(t)s(t)$ ;
- 2) 相加  $W(t) = x(t) + \mu s(t)$ ;
- 3) 加乘结合  $W(t) = x(t)[1 + \mu s(t)]$ 。

其调制技术主要有以下几种:

- 1) 数字混沌调制的有线 (CD) <sup>2</sup>MA 通信。
- 2) 脉冲同步的混沌调制。

参考文献 (略)

作者联系方式

通信地址: 西安市王曲镇西安通信学院研管大队九队  
邮政编码: 710106  
联系电话: 13772161955

- 3) 混沌脉冲定位调制 (CPPM) 的数字通信。
- 4) 无同步的脉冲无线发送的混沌调制。

3.4 比较与分析

上述方法从不同角度对信息进行隐藏加密, 各有其优劣。Baptista 设计的基于搜索机制的混沌密码有两个缺陷, 首先密文分布不是均匀的, 其次每个明文字符至少要迭代  $N_0$  混沌迭代, 这使得其加密速度相对其他传统密码而言太慢了, 从而限制了 Baptista 加密算法的应用。由于 Baptista 密码的缺陷, 人们对其进行了深入研究并提出了改进方法, 其中 Wong 方案和李树钧方案均提高了其加密效率。

对于单向散列的混沌加密而言, 散列在计算的过程中容易发生碰撞, 即给定不同的初值通过散列函数得到的结果是一样的, 所以需要选择合适的散列函数, 对其进行碰撞分析。同时散列能够防止消息被意外改变, 但任何人只要正确的散列函数都可以恢复明文。因此, 散列有助于确保数据不被偶然改变, 但并不能保证数据故意被改变。

基于调制的混沌加密是目前研究的新技术, 具有广阔的前景, 可望在实际的通信系统中发展起来, 但仍存在技术上的难题。主要缺点是通信信道中对噪声的敏感性和畸变性使得混沌加密信号在传输过程中受到噪声影响大, 信号失真比较严重。

4 总结

电子军务是一项复杂的系统工程, 需要安全作为保证, 利用混沌加密技术可提高电子军务的安全性, 防止数据窃取, 为其正常运行搭建一个平稳的平台。在文中分析了三种加密算法, 下一步将对混沌加密在电子军务的具体应用做更深入的研究。

# 两种网管标准的安全性分析

卢宁 王建新 肖刚

**摘 要:** SNMP 是 IP 网中最流行的网络管理工具, WBEM 是由 DMTF 管理的一套网络管理规范, 本文着重分析了这两种网管标准的安全性。

**关键词:** SNMP; WBEM; 网络管理; 安全性

## 1 引言

随着信息技术的发展, 计算机网络在各行各业中有了越来越广泛的应用, 网络管理也随之受到格外的关注。由于要进行网络管理, 必然允许管理员从远程控制被管主机, 那么如何保证管理安全性的问题也就凸现出来。在进行网络管理时, 可能会受到的攻击主要有以下 6 类<sup>[1]</sup>。

1) 伪装 (Masquerade) 威胁。一些未被授权的实体冒充一个授权实体去执行只有授权实体才可以执行的一些管理操作。

2) 信息更改 (Modification of information) 威胁。一些未授权的实体更改所传输的消息的内容, 以致产生非法的网管操作, 如对象查询、系统配置和计费等。

3) 信息泄漏 (Disclosure of information) 威胁。不怀好意的人可以窃听管理代理和管理站之间的信息交换, 从而获得管理对象的值和通告事件。例如, 通过观测更改口令的 set 命令, 可以得到新口令的内容。

4) 消息流更改 (Message Stream Modification) 威胁。IP 网是基于存储转发机制的。因此, 消息或报文的正当排序、时延或转发是很自然的。但是, 有一种威胁可以通过使消息被重排、延迟或重放 (复制), 从而导致越权的管理操作。例如, 一个重新启动设备的消息可以被复制, 并于将来某一时刻重放。

5) 服务拒绝 (Denial of service) 威胁。攻击者可以截取管理代理和管理站之间正常的信息交换消息实施攻击活动。

6) 流量分析 (Traffic analysis) 威胁。攻击者可以分析管理代理和管理站之间的业务流模型。

由于存在以上安全威胁, 各种网管标准在制定

时都考虑了相应的对策, 下面我们将对 SNMP 和 WBEM 这两种不同的网管标准的安全性进行分析和比较。

## 2 SNMP的安全性分析

简单网络管理协议 (SNMP) 发布于 1988 年<sup>[2]</sup>, 至今已经成为 IP 网中最流行的网络管理工具。在将近 20 年的发展过程中, SNMP 产生了 3 个不同的版本。

### 2.1 SNMPv1 的安全缺陷

1990 年, IETF 正式发布了 SNMPv1<sup>[3]</sup>, 并在 90 年代取得了迅猛的发展。SNMPv1 是基于简单原则制定的, 操作起来简单高效, 但同时也暴露了许多缺陷, 如难以实现大量的数据传输, 缺乏安全控制机制。在 SNMPv1 中仅采用一个非常简单的身份认证机制: 使用一个被称为 community name 的字符串来进行身份识别。具有相同的 community name 的管理者 (Manager) 和代理人 (Agent) 称为一个组 (group), 只有组内的成员才能够相互传递管理信息。但 community name 这个字符串在存储及发送的管理信息报文中均没有采取任何保密措施, 因此它很容易被窃取, 而一旦获知了 community name 则可对组内成员 Agent 的 MIB (Management Information Base) 进行操作, 这将对网络安全造成巨大的威胁。在网络规模越来越大, 复杂性和异构性越来越高的今天, SNMPv1 在功能及安全性上的缺陷使得它已无法适应复杂的网络环境。

## 2.2 SNMPv2 的改进和不足

为了克服 SNMPv1 存在的问题, IETF 于 1993 年推出了 SNMPv2<sup>[4]</sup>。它的操作流程如下。

1) 当一个 PDU 需要传送时, 首先要准备一个所谓的 SnmpMgmtCom (SNMPv2 management communication) 值。它包括 dstParty (目的参加者)、srcParty (源参加者)、context (上下文) 和 PDU。

2) 通过参考本地数据库确定发送方的认证协议和相关的参数。如果需要认证协议, 则需要加上目的参加者和源参加者的时间戳 (dst timestamp、src timestamp)。然后, 通过 MD5 算法使用源参加者的私有认证密钥 (src auth key) 计算消息摘要 (digest), 并将其加上。

3) 如果目的参加者需要加密, 则使用 DES 算法将得到的序列加密。加密所用的目的参加者私有密钥 (dst priv key) 可从本地数据库中获取。然后, 在加密后得到的新的序列前加上一个未加密的目的参加者对象标识。

4) 最后, 使用接收方的传输地址和传输域, 把消息序列发送到传输层。

SNMPv2 协议虽然以 SNMPv1 作了重大改进, 采用了身份验证协议和隐私协议, 但由于所使用的算法 DES 和 MD5 均属于单钥加密系统, 因而存在密钥分配问题。SNMPv2 协议本身并未解决该问题; 另外, 参加者概念的使用需要大量复杂配置, 即使为了实现一个简单的功能, 也必须完成所有的配置工作。基于以上原因, 最终 SNMPv2 没有被广泛应用。

## 2.3 SNMPv3 安全性分析

### 2.3.1 SNMPv3 概述

IETF 于 1998 年 1 月发布, 又于 1999 年 4 月改进了 SNMPv3<sup>[5]</sup>。在 SNMPv3 中, 用实体的概念替代了之前的代理和管理者。一个 SNMP 实体既可以是代理也可以是管理者, 或者二者的综合体。由于采用模块化结构设计, 因此每个实体都包含一些功能模块。模块之间相互协调, 共同完成任务。

与以前的版本相比, SNMPv3 并没有改变 PDU 格式, 而是完善了其安全特性。它的安全特性体现在认证和存取控制两个方面。

SNMPv3 基于用户的安全模型<sup>[6]</sup> (USM) 为网

络管理提供了加密和鉴别机制。USM 应用 MD5 或 SHA 对消息进行摘要处理, 将输入消息生成散列值, 以提供身份鉴别和完整性功能。USM 还通过 DES-CBC 加密算法来保证消息的私有性。它提供了 3 种服务: 不鉴别也不加密、鉴别但不加密、鉴别并加密。

SNMPv3 用基于视图的访问控制模型<sup>[7]</sup>来设定用户访问权限。通过考察发出消息的用户、消息的安全级别、消息的请求操作类型等控制用户对 MIB 的访问权限, 并允许远程配置该特性。可以看出, SNMPv3 的访问控制特性为网络管理提供了更有效的安全性。

### 2.3.2 SNMPv3 的安全性能分析

为便于研究 SNMPv3 安全性, 下面的分析中假定其均在既做身份鉴别又加密的安全级别。SNMPv3 属于应用层的协议, 因此它的安全特性也在应用层上实现, 以保证端到端连接的安全性。但这些安全特性不适用于其他的应用。SNMPv3 的标准中只定义了唯一的加密标准, 即 DES-CBC。

要实现 SNMPv3 的安全特性, 需要有比普通 SNMP 更长的消息格式。由于在 SNMPv3 的定义中, 有些内容是不定长的, 如 community string, 因此其消息的长度一般很难确定。但很显然, SNMPv3 要比老版本的 SNMP 占用更多的网络带宽。

除了网络负载方面的影响, 嵌入式的安全特性也会给 SNMPv3 代理带来额外的计算量, 有可能降低网络设备的性能。

SNMPv3 的安全服务可以被用户直接调用, 这意味着用户必须记住密码。有时, 应用一些工具可以为常用的参数定义默认值 (如密码)。但由于密码有可能是以纯文本的方式保存下来的, 因此会引起安全问题。

## 3 WBEM的安全性分析

### 3.1 WBEM概述

1996 年以 Microsoft, BMC Software, Cisco Systems, Compaq Computer, Intel 为首的一些公司联合提出基于网络的企业管理<sup>[8]</sup> (Web-Based Enterprise Management, 简称 WBEM) 计划, 随后

为了 WBEM 标准的更快发展和推广，他们将其交给了分布式管理任务组（Distribute Management Task Force, DMTF），然后这些创始公司与在 DMTF 一起，开发了一套独立于环境的规范原型，用于描述和访问所有类型的管理规范。

WBEM 的核心思想是对所有被管对象以受管对象格式（MOF）进行统一建模，这些模型称为公共信息模型<sup>[9]</sup>（CIM），存放在 CIM 库中通过一个 CIM 对象管理器提供给管理应用程序调用。可以说 WBEM 规范建立了一个工业标准，使管理者可以使用任一个浏览器管理分布的网络、系统和应用。因此，WBEM 为网络管理员提供了极大的方便，使管理员可以用一个统一的接口管理网络中多样的设备和主机系统中的应用程序。

WBEM 并没有定义新的通信协议，而是使用 HTTP 协议来传输经过 XML 编码的 CIM 消息<sup>[10]</sup>。一个 CIM 消息就是一个定义良好的请求或响应数据包，用于在 CIM 产品间交换信息。目前有两种类型的 CIM 消息：CIM 操作消息和 CIM 输出消息。

CIM 操作消息用于在目标名称空间上调用一个操作。

CIM 输出消息用于和外部的名称空间或元素通信。CIM 输出消息仅仅是一个信息，它并不定义目标名称空间上的操作，甚至并不意味着目标名称空间确实存在。

CIM 消息的语法和语义是以一种不受具体协议封装约束的方式进行描述的，XML 是这种描述的基础。

## 3.2 WBEM关于管理安全性的措施

### 3.2.1 CIM角色验证

CIM 服务器可以返回 CIM 角色验证首部，它作为 401 未经授权响应的一部分，和 WWW 验证首部在一起。CIM 角色验证首部有一个口令集来指明 CIM 服务器关于角色证书有哪些策略。

challenge = "credentialrequired" | "credentialoptional" | "credentialnotrequired"

credentialrequired 表示 CIM 服务器要求如果 CIM 客户端想要假冒一种角色，那么必须提供证书。

Credentialoptional 表示证书是可选的。这种情况下，CIM 服务器允许无证书的访问，但是某些需

要角色证书的操作可能无法成功。

Credentialnotrequired 表示为了假冒该角色，不需要证书。

没有 CIM 角色验证首部表示 CIM 服务器不支持角色假冒。CIM 客户端应该适当地处理这种情况。

口令不包含任何授权模式、领域或者其他信息。CIM 客户端应该从 WWW 验证首部中获取这些信息。这意味着对于任何给出的请求，角色证书应该使用与用户证书相同的模式。

仅当用户被允许假冒角色时，CIM 服务器才允许角色假冒。这意味着即使提交了适当的证书，角色假冒也可能失败。如果用户验证和角色假冒均告失败，那么整个验证操作失败。

### 3.2.2 CIM角色授权

该首部连同一般授权首部一起提供，以便 CIM 客户端进行用户验证。如果 CIM 客户端希望进行角色假冒，并且服务器口令是“credentialrequired”，那么 CIM 角色授权首部必须提供适当的证书。提供的证书作为 CIM 角色授权首部的一部分，必须遵循 RFC2617 中关于授权首部的规定。这样一来，对于角色证书基本的和摘要的验证都将成为可能。

当服务器口令是“credentialoptional”或“credentialnotrequired”时，如果 CIM 客户端希望假冒某一角色但不提供任何角色证书，那么 CIM 角色授权首部必须按照 RFC2617 的规定设置“auth-scheme”域为“role”，其中“auth-param”参数必须包含角色名称。

无论是否预期得到证书，CIM 服务器必须有处理能力处理 CIM 角色授权首部里的证书。当然，它也可以选择忽略这些证书。

## 3.3 HTTP协议的安全性

由于 WBEM 规范使用 HTTP 协议作为其传输协议，因此，HTTP 协议的安全性也对其管理安全性起着重要作用。HTTP 的验证方法有基本验证和摘要式验证两种模式<sup>[11]</sup>。

基本验证提供了一个非常初级的验证级别，它的最大的弱点是客户端口令以明码传输。因此，除非在一个高度安全的环境中（例如在使用 SSL 的连接中，或者在物理上确保安全的私有网络中），

否则 CIM 客户端、服务器、监听器都不能使用基本验证, CIM 服务器和监听器不能发送基本验证的证书。

摘要式身份验证采用的是一种请求/响应的机制, 它在网络上发送摘要 (hash), 而不发送密码。在摘要式身份验证期间, IIS 向客户端发送请求以创建一个摘要, 然后将该请求发送给服务器。然后, 客户端发送一个基于用户密码和数据 (对于客户端和服务端都是已知的) 的摘要, 作为对请求的响应。服务器使用与客户端相同的过程创建自己的摘要, 其用户信息获取自 Active Directory。如果服务器创建的摘要与客户端创建的摘要相匹配, 则 IIS 将认为客户端通过了身份验证。摘要式身份验证的局限性是它只能在 Active Directory 域部署中使用。尽管摘要式身份验证比基本验证要安全不少, 但是仍然是可以受到攻击的。攻击者可以记录

客户端和服务端之间的通信, 然后使用此通信信息重播该事务。

管理应用程序应该支持摘要验证模式。因为摘要验证不使用明文发送密码, 至少它比基本验证安全得多。然而, 那些需要更加健壮的保护的 CIM 客户端、服务器和监听器, 应该使用诸如 SSL (加密套接字协议层) 或 SHTTP 之类的加密机制。

## 4 结束语

IP 网存储转发的基本特征决定了在 IP 网中没有绝对的安全, 而协议安全性的提升必然提高其复杂程度, 从而降低了处理速度。安全和性能是一对矛盾, 在实际使用中, 我们必须对其进行综合考虑。

## 参考文献

- [1] 应伟峰, 段晓东, 沈金龙. 简单网络管理协议的安全性分析. 南京邮电学院学报 (自然科学版), 2002, 22 (1) .
- [2] A Simple Network Management Protocol. IETF RFC1067. August, 1988.
- [3] A Simple Network Management Protocol (SNMP). IETF RFC 1157. May, 1990.
- [4] IETF RFC 1442~1450. April, 1993.
- [5] IETF RFC2571~2573. April, 1999.
- [6] User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). IETF RFC 2574. April, 1999.
- [7] View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). IETF RFC 2575. April, 1999.
- [8] Web-based Enterprise Management. <http://www.dmtf.org/standards/wbem/>.
- [9] Common Information Model (CIM) Standards. <http://www.dmtf.org/standards/cim/>.
- [10] Specification for CIM Operations Over HTTP. <http://www.dmtf.org/standards/wbem/>
- [11] HTTP Authentication: Basic and Digest Access Authentication. IETF RFC 2617. June, 1999.

## 作者联系方式

通信地址: 北京市丰台区大成路 13 号 W03

邮政编码: 100039

联系电话: 010-66820399

# 军用Ad Hoc信息网络的安全威胁及对策

鲁岩 程磊 王晨晖

**摘 要:**近年来,随着民用信息技术的军事领域的广泛运用,军用信息网络的开放性对军事信息的安全带来了一定的影响,并制约着我军信息化建设整体步伐的进行。因此,在充分利用成熟的民用信息网络技术的同时,注重对于信息网络安全的管理与建设是我军信息化发展过程中的一个重要问题。

**主题词:** Ad Hoc; 无线信息网络; 安全威胁

20 世纪 90 年代末以来,民用的 Ad Hoc 网络经过改进与发展,已经在军用信息网络中得到了一定程度的运用,而这种运用的趋势,随着民用技术民用化的深入,也在不断的发展。同时,由于民用信息网络技术的开放性高、通用性好、介入性强等特点,其安全性一直是影响其在军事领域快速运用的一个重要问题。因此,Ad Hoc 信息网络的安全性是决定其潜能能否得到充分施展的一个关键所在,特别是 Ad Hoc 网络在高密级军事通信网络中的运用。由于 Ad Hoc 网络不依赖固定基础设施,为其使用的安全体系结构提出了新的挑战,相比于传统的网络,Ad Hoc 网络更易受到各种安全威胁和攻击,包括被动窃听、数据篡改和重发、伪造身份和拒绝服务等。用于传统网络的安全解决方案不能直接应用于 Ad Hoc 网络,现存的用于 Ad Hoc 网络的大多协议和提案也没有很好解决安全问题,特别是没有考虑特定的环境。

## 1 在信息化战场上Ad Hoc网络的安全问题

在传统网络中,网络采用层次化体系结构,主机之间的连接是准静态的,具有较为稳定的拓扑,可以提供多种服务来充分利用网络的现有资源,包括路由器服务、命名服务、目录服务等。现在,已经提出了一系列针对这类环境的安全机制和策略,如加密、认证、访问控制和权限管理、防火墙等。Ad Hoc 网络不依赖固定基础设施,具有灵活的自组织性和较强的健壮性。Ad Hoc 网络中没有基站或中心节点,所有节点都可以移动、节点间通过无线信道建立临时松散的连接,网络的拓扑结构动态

变化。Ad Hoc 网络由节点自身充当路由器,也不存在命名服务器和目录服务器等网络设施。根据应用领域的不同,Ad Hoc 网络在体系结构、设计目标、采用的协议和网络规模上都有很大差别。尽管基本的安全要求,如机密性和真实性,在 Ad Hoc 网络中仍然适用。但是 Ad Hoc 网络不能牺牲大量功率用于复杂的运算,并要考虑无线传输的能耗和稀少无线频谱资源。另外,节点的内存和 CPU 功率很小,强安全保护机制难以实现。这些约束在很大程度上限制了能够用于 Ad Hoc 网络的安全机制,因为安全级别和网络性能是相关的。因此,传统网络中的许多安全策略和机制不能直接用于 Ad Hoc 网络,需要对现有的安全措施加以改进,并采用新的安全策略和方法,因此限制了 Ad Hoc 网络整体作战性能的提高。Ad Hoc 网络的安全目标与传统网络中的安全目标基本上是一致的,包括:数据可用性、机密性、完整性、安全认证和抗抵赖性。

### 1.1 可用性

可用性是指即使受到攻击,节点仍然能够在必要的时候提供有效的服务。可用性保证网络服务操作正常并能容忍故障,即使存在拒绝服务共计的威胁。在军事领域,Ad Hoc 网络的可用性涉及多层,如在网络层,攻击者可以篡改路由协议,例如在战场上将 Ad Hoc 网络流量转移到无效的地址或关闭网络;而在通话安全管理层,攻击者可以删除会话级安全信道中的加密;在应用层,密钥管理服务也可能受到来自战场的网络攻击和威胁等。



## 1.2 机密性

机密性是 Ad Hoc 网络在工作过程中能够保证特定的信息不会泄露给未经授权的用户。在信息化战争中,军事情报或用户身份认证等安全敏感的信息在网络上传输时必须机密、可靠,否则这些信息被敌方或恶意用户捕获,后果将不堪设想,而这个问题的解决需要借助于认证和密钥管理机制。

## 1.3 完整性

完整性保证信息在 Ad Hoc 网络发送过程中不会被中断,或者阻塞,并且保证节点接收的信息应与发送的信息完全一样,确保战场信息传输的真实性与可靠性。如果军用的 Ad Hoc 网络没有完整性保护,网络中的恶意攻击或无线信道干扰都可能使信息遭受破坏,从而变得无效,进而使依赖于这个网络的信息传输全部中断。

## 1.4 安全认证

Ad Hoc 网络的安全认证就是指每个节点需要能够确认与其通信的节点身份,同时要能够在没有全局认证机构的情况下实施对用户的鉴别。如果没有严密、可靠的认证,在战场上敌方攻击者很容易冒充某一节点,从而得以获取重要的资源和信息,并干扰其他节点的通信,使得整个网络的效率大大降低或者是失去效用。

## 1.5 抗抵赖性

Ad Hoc 网络的抗抵赖性用来确保一个节点不能否认它已经发出的信息,它对检查和孤立被占领节点具有特别重要的意义,在战场上,当一个信息节点接收到来自被占领节点的错误信息时,抗抵赖性保证未被占领或者破坏的节点能够利用该信息告知其他网络节点,该节点已被占领,进而使整个网络能够迅速的对该节点进行屏蔽,使对方不能通过该节点,截取 Ad Hoc 网络的整体信息,也就保证了战场信息的安全与指挥控制的稳定。

# 2 信息化战争中Ad Hoc网络的安全策略和机制

针对 Ad Hoc 网络的弱点,各国都积极地开

展确保网络信息安全的研究与相关技术和机制的开发,传统的安全机制,如认证协议、数字签名和加密,在实现 Ad Hoc 网络的安全目标时依然具有重要的作用,是当前军用 Ad Hoc 网络的安全保障的重要手段。

## 2.1 防止信息窃取攻击

在军事领域,由于使用多跳的无线链路使 Ad Hoc 网络很容易受到诸如被动窃听、主动入侵、信息假冒等各种信息窃取攻击,战场信息安全受到了严重的威胁。被动窃听可能使敌方获取保密信息,主动窃取攻击中敌方可以删除有用信息、插入错误信息或修改信息,从而破坏了战场数据的可用性、完整性、安全认证和抗抵赖性。对付被动窃听攻击,可以根据实际情况采用 IPSec 中的安全套接字协议(SSL)或封装安全净荷(ESP)机制。封装安全净荷可以为不能支持加密的应用程序提供端到端的加密功能,它不仅可以对应用层数据和协议报头加密,还能对传输层报头加密,从而可以防止攻击者推测出运行的是那种应用,具有较好的安全特性。同样,在战场上为对付针对 Ad Hoc 网络的主动攻击,可以采用带有认证的端到端加密的方法。

## 2.2 加强路由协议安全

在信息化战争中,目前使用的多数 MANET 路由协议能够适应网络环境的快速变化。由于路由协议负责为节点指定和维护必要的路由结构,必须防止机密性、真实性、完整性、抗抵赖性和可用性的攻击。在战争中,如果 Ad Hoc 网络的路由协议受到恶意攻击,整个 Ad Hoc 网络将无法正常工作。所以,必须提供相应的安全机制,以便保护 Ad Hoc 网络路由协议的正常工作。但是,目前军用 Ad Hoc 网络中的路由协议大都没有考虑这个问题,使得其安全与稳定性一直难以得到充分的提高。未来战争中,特别是在开放的战场环境中保护路由流量是非常重要的课题,以便通信各方的身份和位置不被未授权的实体所了解,因此,路由信息必须防止认证和抗抵赖性攻击,以便验证数据来源的安全与可靠。

当前,军用 Ad Hoc 网络路由协议的安全威胁主要来自两个方向。

### 2.2.1 网络外部信息攻击

主要是指来自网络外部的攻击者通过发送错误的路由信息、重放过期的路由信息、破坏路由信息等手段，来达到致使网络出现分割、产生无效的错误路由、分组无谓的重传，网络发生拥塞并最终导致网络崩溃的目的，恶意攻击者还可以通过分析被路由业务流量来获取有用信息。

### 2.2.2 网络内部信息攻击

主要是指网络内部的攻击者可以向网内其他节点发布错误的路由信息和丢弃有用的路由信息，进而使整个网络陷入瘫痪，或者是效能降低。

网络外部信息攻击、网络内部信息攻击两种攻击方式都能造成网络中合法节点得不到应有的服务，因此，也可以看作为一种拒绝服务的网络攻击。在实际运用中，使用者常常可以使用数据安全中的各种加密机制来解决第一种威胁，如带有时间戳的数字签名；而解决第二种威胁较为困难，对路由信息进行加密的机制不再可行，因为被占领的节点可以使用合法的私有密钥对路由信息进行签名。

## 3 在信息化战场上保障Ad Hoc网络安全的主要措施

### 3.1 访问控制

在军用的 Ad Hoc 网络中与民用的 Ad Hoc 网络同样存在控制对网络的访问以及控制访问网络提供的服务的需求。在网络层，路由协议必须保证不允许非授权节点加入网络，保证没有敌对节点加入和离开网络而不被检测到；而在应用层，访问控制必须保证非授权用户不能访问服务。访问控制常与身份识别和认证相关联，确保合法用户有权访问服务。在一些系统中可能不需身份识别和认证，节点通过证书来访问服务，而根据不同的网络结构和安全级别，访问控制的实现方式也不同，集中式的低安全级别网络，可以采用服务器控制的方式确保网络的整体安全。

### 3.2 网络操作和服务的安全性

军用 Ad Hoc 网络的安全操作需要对链路或网络层进行保护。在一些解决方案中，链路层提供强

安全服务用以保护机密性和真实性，在这种情况下高层所需的安全要求会减少。对于 Ad Hoc 网络的军事应用，机密性尤其重要，没有位置、身份和通信的保护，军事领域的 Ad Hoc 网络中的用户非常容易遭受各种攻击，如果网络的可用性遭到破坏，用户可能根本无法执行他们的任务。路由信息的真实性和完整性常常并行进行处理，如果使用的是公钥密码体系，可以采用数字签名来证实数据的来源和完整性。抗抵赖性某种程度上与真实性（认证）相关，路由流量必须留下记录，使得发送路由信息的任何方都不能随后否决它向其他方传送了数据。

### 3.3 网络安全认证

军用 Ad Hoc 网络在不同的战场环境可以采用不同的认证机制，以提高其安全性和稳定性。在实际运用过程中，常常通过使用便携式电脑组建 Ad Hoc 网络来召开临时作战会议的应用环境中，使得与会者彼此之间通常比较熟悉并彼此信任，会议期间他们通过手提电脑通信和交换信息。在此种网络环境和工作情况下，Ad Hoc 网络的终端使用者可能没有任何途径来识别和认证对方的身份，因为，此时 Ad Hoc 网络的终端使用者既不共享任何密钥也没有任何可供认证的公共密钥。在这种工作环境中，敌方网络攻击者可以窃听并修改在无线信道上传输的所有数据，还可能冒充其中的 Ad Hoc 网络的终端使用者。为了保障 Ad Hoc 网络在此种较为开放的工作环境中的安全与稳定，通常可以采用基于口令的认证协议（PBA），因为此种认证协议，继承了加密密钥交换协议（Encrypted Key Exchange）的设计思想。在 PBA 协议下的工作环境中，所有的 Ad Hoc 网络的终端使用者都参与会话密钥的生成，从而保证了最终的密钥不是由极少数使用者产生的，攻击者的干扰无法阻止密钥的生成。同时，PBA 协议还提供了一种完善的口令更新机制，Ad Hoc 网络的终端使用者之间的安全通信可以基于动态改变的口令来建立。按照这种方式，即使攻击者知道了当前的口令，也无法知道以前的和将来的口令，从而进一步减少了战场信息泄密的概率。

### 3.4 信任问题

在网络安全相对脆弱的 Ad Hoc 网络应用环境中，特别是在战争中由于节点容易受到攻击，被俘

获的可能性也较大,因此必须要建立适当的信任机制。在 Ad Hoc 网络中,信任问题是中心问题,而要解决这个问题必须借助密钥。因此,一个基本的问题是如何生成可信任的密钥而不依赖受信任的第三方。军用的 Ad Hoc 网络是一个动态自组织临时网络,不能保证网络中各个节点持有被其他节点信任的公钥,并且它们也无法出示可以互相信任的证书,一种策略是允许节点之间委托信任,已经建立信任关系的节点能够向组中其他成员扩展这种信任。

### 3.5 密钥管理

在网络安全领域,与任何其他分布式系统一样,正确的使用密钥管理系统对于军用 Ad Hoc 网络的安全性十分重要。因此,使用者需要一种与情景相关的高效的密钥管理系统,对于快速变化的 Ad Hoc 网络,密钥的交换可能需要按需进行而不能假设实现协商好的密钥,而对拓扑变化较慢的小型 Ad Hoc 网络,密钥可以进行协商或手工配置。

在战场上,如果 Ad Hoc 网络的终端使用者采用公钥体系,整个保护机制依赖于私钥的安全性,而此时由于节点的物理安全性较低,私钥必须秘密地存储在节点中,例如使用一个系统密钥加密。但是这并非一个动态的 Ad Hoc 网络希望的特征,因此需要正确的硬件保护或者将密钥分布到多个节点。Ad Hoc 网络中,数据的完整性和抗抵赖性一般也需要基于某种加密算法来实现,在军用的 Ad Hoc 网络中,加密协议总体上可以分为私有密钥机制(如 DES 和 IDEA)和公开密钥机制(如 RSA)两类。但是,其在战场上实际面临的挑战是密钥的管理,如果采用私有密钥机制,则每个需要通信的节点之间都需要一个秘密密钥,所需管理的密钥数目为  $N(N-1)/2$ ,其中  $N$  是节点数。对于规模较大的军用 Ad Hoc 网络而言,就难以实施有效的密钥管理。因此,通常采用公开密钥机制,但是由于没有中心节点和证书机构,密钥的管理仍很困难,而其中的一种解决密钥管理的方法是使用用户团体来代替证书权威机构,并在节点中分配证书目录。

### 参考文献

- [1] Dean E. B., Unal R., Elements of designing for cost. Proceedings of AIAA 1992 Aerospace Design Conference, February, 1992, Irvine, CA.
- [2] [美]阿瑟·塞布罗夫斯基.《军事转型与不断变化的战争特点》.《外国军事学术》2004 年第 11 期
- [3] [美]道格拉斯·麦克格瑞高尔.《陆军转型:对未来的假设》.2004 年在美国会武装力量委员会上的报告

### 作者联系方式

通信地址:海南海口市海南省军区装备部

邮政编码:570236

联系电话:0898-66571655 13876765315

# 浅谈我军信息网络安全保障建设

罗敏

**摘要：**本文分析了我军信息安全建设的现状和存在的问题，讨论了我军信息安全保障体系建设目标。

**关键词：**多层次；安全保密

## 1 概述

在我军新型战斗力标准中，着眼提高“四个能力”：突出抓好以一体化信息支持能力为核心的信息系统建设，以信息化火力打击能力为核心的武器装备信息化建设，以多层次信息作战能力为核心的信息对抗建设，以系统防护和信息安全保密为主的全方位综合防护能力建设。可见，推进我军的信息安全安全保障建设是提高我军战斗力关键环节之一。

信息网络存在的攻击包括：非法者的被动攻击（窃听、破译）和主动攻击（中断、截取、修改、伪造、冒充等）。另外，合法用户和管理人员的误操作也会对信息安全性、完整性和可用性造成破坏，也应视为一种攻击<sup>[1]</sup>。

敌对攻击者通常使用的是“最易渗透原则”，即系统中最薄弱而不是最坚固的地方最容易遭受攻击；系统本身在物理上、操作上和管理上的种种漏洞构成了系统的脆弱性。尤其是网络系统自身的复杂性、资源共享性使单纯的安全技术防不胜防。水会从木桶最低的木板流出来，不论其他木板块有多高。增强免疫力和抵抗力总比“头痛医头、脚痛医脚”好，同样，预先发现并堵住系统的漏洞比想当然地“加固”已有的安全技术和措施更重要。任何低估攻击者水平和实力的想法都是危险的。

## 2 国内外战术网络信息安全保障现状

### 2.1 国外现状

为加强信息安全保障建设，美国推出了一系列措施和政策。发布了《信息保障技术框架》，建立军兵种信息系统安全办公室。加大投入实施密码现代化计划，并建立了《GIG 信息保障政策和实施指

南》。拟定了《国防信息系统安全计划》，在全球指控系统 CCS，国防信息系统网 DISN，武士 C4I 等系统中提供了多级信息系统安全保障措施<sup>[2]</sup>。

俄军将网络—信息战称为“第六代战争”，认为在未来战争中，要夺取并掌握制信息权和制电磁权，就必须打赢网络—信息战。为此，俄军制定了网络安全法规，同时加强对网络的侦察与安全检查。另外，日本、韩国、英国、印度也都在为打网络战作准备。目前，印军正拟组建网络战部队，以打响虚拟空间的争夺战即网络战。

### 2.2 国内现状

在信息安全方面，我军也与世界各国一样，首先关注的是通信信息的保密，然后是通信网络的安全与保密。我国信息系统安全保密设备已基本自成体系，基本保证了从中央到各军兵种以往军事信息的安全与保密。

但总体而言，我军的通信保密水平落后于世界上许多先进的国家。

新的军事技术革命和信息战的提出，促使我军军用信息的安全保密也由信息传输保密向多业务/多媒体/多种传输方式下的计算机化、网络化、综合化的安全与保密的转变。多种密级、多种类别信息要能通过一个综合信息系统进行处理和传送，有鉴于此，我军信息安全保密方面仍存在一系列弱点和差距，难以适应新形势下的作战要求。

## 3 我军信息安全保障建设中存在的问题

### 3.1 认知误区

#### 3.1.1 加密=安全

密码学尽管在网络信息安全中具有举足轻重的

作用,但密码学绝不是确保网络信息安全的惟一工具,它也不能解决所有的安全问题。同时,密码编码与密码分析是一对矛盾和盾的关系,俗话说:“道高一尺,魔高一丈”,它们在发展中始终处于一种动态的平衡。在网络信息安全领域,除了技术之外,管理也是非常重要的一个方面。如果密码技术使用不当,或者攻击者绕过了密码技术的使用,就不可能提供真正的安全性。

### 3.1.2 安全保密滞碍通信

层出不穷的各种病毒、木马及各种其他拒绝服务攻击手段,显而易见,已严重影响了当今各种信息网络的效率和信息安全。信息安全保密作为通信系统的保障,合理利用,在一定程度上能够促进通信的发展,并保障通信效率。

由于我国基础设施和核心技术方面的薄弱,致使我军通信系统通信能力相对较低(指战术通信网络部分),网络可靠性较差。各通信系统研制单位往往认为信息安全防护会降低通信效率,增大通信时延,降低通信可靠性,滞碍通信系统的发展,大部分通信系统研制阶段,未将信息安全防护纳入统一规划和设计,致使我军现役通信系统不得不以补丁方式,堆砌各种安全防护手段,而各防护系统只能烟囱式发展,导致大量的重复、冗余设计,严重影响信息安全保障的建设。

## 3.2 建设过程中误区

### 3.2.1 装饰性建设

有关军用信息安全重要性的认识还有待进一步加强。以往,不管是管理机构还是信息用户,对于信息安全常自觉不自觉地有着“说起来非常重要,做起来可以不要”的矛盾表现,把安全当作信息系统的累赘和不情愿的负担。就是在资金不算十分匮乏的情况下,也有限制安全投入的倾向。这不可能不弱化系统安全的建设。

### 3.2.2 滞后建设

目前,我军各型综合业务信息网络都缺乏一体化的系统安全性设计,信息处理与网络通信的安全设计尚未统一,彼此脱节。

要坚决克服那种先把网络建起来,解决了“有”的问题之后,再去考虑信息安全保密问题的错误认识。注意从系统的整体性出发,统筹考虑,同步进行,协调发展。须知,一个没有信息安全技

术屏护的网络,一个完全开放透明和裸露的网络,有不如无。没有安全优势,就没有网络优势,没有网络优势,就没有信息优势,没有信息优势,建设信息化军队,打赢信息化战争就将成为一句空话。

## 3.3 基础薄弱

### 3.3.1 缺乏自主基础性平台和核心技术

芯片作为基础性平台,是实现信息安全的根本,我国在这些基础工业方面相当薄弱;各种处理平台、操作系统、应用支撑系统、通信协议等核心技术,基本都掌控在西方国家手中,我国主要靠国外引进,存在很大的安全隐患<sup>[3]</sup>。这些因素无疑影响到信息安全防护体系的建立。

### 3.3.2 管理不完善

我军目前没有形成系统的信息安全管理体制,信息安全法律制度尚未形成体系。各机构管理制度尚未完全建立,职责不明确。我军缺乏总体的军用信息安全的远、中、短期实施计划等等。

### 3.3.3 安全意识淡薄

要确保信息的完整性、可用性和保密性,当前最为紧要的是各级都要确立信息网络安全战略意识。必须从保证信息安全,就是保证国家主权安全,掌握军事斗争准备主动权和打赢信息化战争主动权的高度,来认识信息网络安全的重要性。应当着重强调:在进行国家和军队信息化建设时,要大力开发各种信息安全技术,普及和运用强有力的安全技术手段。技术的不断创新和进步,才是信息安全的關鍵,才是实现信息安全最重要、最有力的武器。

## 3.4 缺乏实战演练

虽然我军信息安全建设取得了一定的成就,但信息安全建设必须通过实践的检验。由于我军长期处于和平时期,信息系统未经任何实战考验。无法模拟实战环境,存在诸多未知威胁因素。尽管我国也力求通过演习检验建设成果,但是由于我军通信网络较为落后,军事演习中存在虚假不实成分,不能真正反映敌我信息对抗的实际环境。从总体上看,我军信息安全保障发展还处于初级阶段,处于“单兵”作战、静态防护、被动防御阶段。目前急

需对我军信息安全保障建设进行总体规划、明确保障目标、原则。

4 我军信息安全保障建设设想

限制敌人对信息的利用，确保己方信息渠道的畅通，掌握信息主动权，是我军信息安全保障建设的目的，是信息作战的重要安全屏障。

我军信息安全保障建设处于起步阶段，需要循

序渐进、因势而建，不能一刀切。目前，我军正在加大新一代通信网络的建设，为信息安全保障建设提供平台和环境，信息安全建设必须从通信系统顶层考虑，一体化设计，而对于现役通信网络必须在信息安全总体设计原则下，遵循统一框架，逐步完善。信息安全保障体系从法律法规、技术、管理、组织四层，构建信息安全保障体系，信息安全保障体系如图1所示。

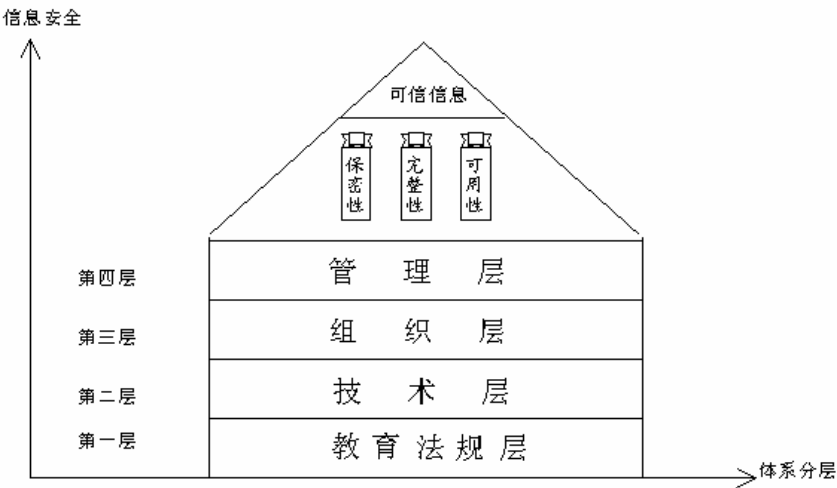


图1 信息安全保障体系

4.1 我军信息安全教育体系

首先，利用全社会的信息安全教育，如办学（大学设信息安全专业、信息安全司法专业）、办班（法规学习班、信息安全基础技术学习班等），培养信息安全人才，利用各种媒体宣传信息社会公德、褒扬守法、挞伐违规，等等。

不仅对国防信息系统及其信息的安全起奠基作用，也是全国的信息安全的基石。

其次，完善信息安全法制体系，做到有法可依，有章可循。国家军委、各军兵种发布的、跟国防信息、信息系统有关的法规、政策和军纪等，它们对保护国防信息系统及其信息安全起着震慑、规范和引导作用。

4.2 组织体系

我军信息安全保障的组织体系，是建立我军的技术服务队伍，保障信息安全防护系统运行有序、高效。主要包括安全管理控制中心、应急协调中

心、安全服务组等。

安全管理控制中心：由安全管理人员组成，主要职责为制订安全管理策略、行政管理制度；负责安全设备的运行监控，检测网络的安全状态，修改网络安全策略等。

应急协调中心：应急响应需要依赖经验和相关知识、数据完成突发事件处理，而且要求的技术繁杂，因此仅仅依赖单一的应急响应组织并不能完全解决问题，必须建筑包括产品提供商、安全专家等在内的应急响应组织保障体系，才能提供有效的应急响应服务，并进行相关技术研究。

安全服务组：为信息系统运转中遇到的信息安全问题提供服务。

4.3 管理体系

管理体系是信息安全保障体系的重要组成部分，完善的管理系统，能够强化管理职能，加强我军信息安全保障的综合协调，优化各项网络安全防

护效能，优化信息安全保障建设。

管理体系主要包括管理规范制度的制定、安全培训、安全服务、安全检查等四项管理内容。

它涉及行政管理安全和技术管理安全。

● 行政管理安全

- 管理机构的确认及其安全管理
- 人事（管理人员、操作人员等）的安全管理
- 网络软硬件安全使用的行政管理
- 军用安全标准、军用安全产品推广应用的行政管理

- 网络扩容的安全规划与管理
- 网络及其安全运行的保卫，等等。

● 技术管理安全

- （多级安全）用户鉴别技术的管理安全
- （多级安全）加密术的管理安全
- 密钥管理术的安全
- 审计/告警术的管理安全
- 设备维护技术的管理安全，等等。

4.4 技术体系

先进的安全技术适应通信网络的特点，是信息安全的基本保障。信息安全保障技术体系从密码保密、安全防护、安全监控、应急保障、安全评估四个环节完成对我军信息网络的多层次、全方位、动态、不断增强的安全保障<sup>[4]</sup>。

安全防护：采用相关安全技术、安全机制、安全产品，以完成信息系统安全体系结构在可认证性、机密性、完整性、可用性以及抗抵赖性五个方面的安全作战使命，提供系统级的安全防护能力。

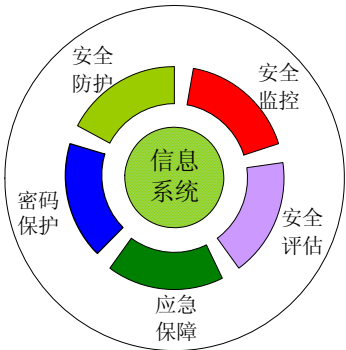


图2 信息安全保障技术体系

安全监控：各级安全监控系统对整个安全防护过程进行监控，它首先从安全防护系统中的安全态势感知系统获取系统的安全态势信息和安全事件数

据，再结合专家系统全方位对收集来的数据进行融合、分析、判断，从而作出决策，协调各安全系统进行联动、作出相应反应。

安全评估：定期对系统的安全机制、安全产品、安全状态进行测试和评估，及时发现其存在的安全脆弱性，并进行公正的评估。测试评估与安全检测是保障信息安全性的关键动态措施<sup>[4]</sup>。

应急保障：对突发事件进行快速反应，尽可能减少突发事件对系统的影响，保证系统安全的最小资源集合可用。当系统遭受毁坏时，评估系统损失情况，在最短时间内恢复系统数据和系统服务，使系统迅速恢复基本的服务。应急响应能力和恢复能力是信息系统生存性、抗毁性的重要衡量标准。

密码保护：完成机要信息传输、处理和存储的加密工作。

通过完善我军信息安全保障技术体系，最终实现从传统的单一防护、静态防护、被动防御模式到多层次立体防护、动态防护和主动防御模式的根本转变。

(1) 多层次防护

在军事信息网络中，同时部署防火墙、防病毒、入侵检测和加密等多种安全防护机制，并通过统一的安全策略，协同工作，构成多层次安全防护的状态，实现安全防护的联防联控、无缝保护。

(2) 动态防护

信息安全已不再是静态的防护，而是一个综合防护、检测、响应和恢复的动态反馈过程。一个良好完整的动态安全体系，不仅需要恰当的防护（如操作系统访问控制、防火墙、加密等），而且需要动态的检测机制（如入侵检测、漏洞扫描等），在发现问题时及时进行响应，成了一个完备的闭环自适应防护体系。

(3) 主动防护

被动式的安全防护技术主要基于特定威胁或攻击的特征，主要在于减轻损失和事后恢复，但却不能从根本上解决安全问题，属于事后“打补丁”的防护。

基于主动安全防护主要在于攻击发生之前就对其进行识别和阻断，识别未知攻击，甚至对攻击者进行主动地取证和进攻。如基于统计的入侵检测系统，可以在攻击发生之前进行预警，识别未知攻击；又如蜜罐网络，可对攻击者进行诱骗，在攻击者毫不知情的情况下对其攻击行为进行取证。

## 5 结论

我军信息安全保障体系建设的目标，是建成顶层综合设计的、一体化多级安全保密的大网。为保

障我军信息的产生、获取、处理、传送和利用全过程的安全，必须有法规、管理、教育等的配合，同时要尽可能地以效费比合算的一切安全保密技术作为有力的支撑。

### 参考文献

- [1] “Mission, Requirements, Threat Analysis for Advanced Telecommunications and Information Distribution Research Program (ATIRP) Interim Report”, 1996, Sanders, A Lockheed Martin Company
- [2] “美俄等国信息战理论与实践的最新发展”，电子信息快报第 55 期，中国电子科技集团第三十所
- [3] “信息安全技术现状与发展”，电子信息快报第 44 期，中国电子科技集团第三十所
- [4] “IT ARCHITECTURE FOR HOMELAND SECURITY”，MILCOM2005, Gerald S. Metz

### 作者联系方式

通信地址：中国电子科技集团公司第三十研究所

邮政编码：610041

联系电话：028-85169767



# 一种基于代理机制的RBAC模型

任毅 肖治庭

**摘要:** RBAC 已经受到信息安全领域的广泛关注。本文在深入研究 RBAC 的基础上, 提出一种基于代理机制的访问控制模型, 称为 DBAC (Deputy-Based Access Control Model)。通过使用代理机制, 该模型支持多粒度、多步灵活的授权机制和多选择的授权回收机制。

**关键词:** 代理机制; 基于角色的访问控制; 访问控制模型; 信息安全

## 1 引言

基于角色的访问控制 (RBAC)<sup>[1]</sup>既能象自主访问控制 (DAC) 那样逐项说明主体对客体的访问权限, 也能象强制访问控制 (MAC) 那样对使用授权进行限制, 因而受到广泛关注。该模型不直接指定用户对客体的访问权限, 而是指定每个角色对客体的访问权限。在此基础上, 通过将用户指派到不同的角色中, 完成对用户的权限指派。用户可以在不同的场景激活不同的角色, 多个用户能同时选定同一角色。该模型具有授权管理简单化, 特权最小化等特点。

然而, RBAC 模型也存在一些问题, 不能很好地满足军事信息系统的某些需求。例如, RBAC 模型要求角色层次满足偏序关系, 上级角色能完全继承下级角色的各项权限。这在很多情况下并不符合实际情况。其次, 安全管理员和高级用户在某些意外情况下 (如外出或生病) 需要请其他用户代行他们的某些权限。本文结合代理机制, 提出一种基于代理机制的访问控制模型 (DBAC) 来解决这些问题。该模型以统一的方式实现各种粒度的权限继承 (以下称为多粒度代理), 并支持权限的多步传递 (以下称为多步代理)。

## 2 相关研究工作

RBDM 模型<sup>[2]</sup>是第一个尝试处理人—人之间基于角色的委托模型。在 RBDM 模型中, 使用 `can_delegate` 条件作为前提条件来限制委托的范围。委托单元是“角色”, 委托的意思是“委托人”给“被委托人”某种角色。然而, 在该模型

中, 委托人不能只委托一部分角色给被委托人, 也不能打破一个角色。

PBDM 模型<sup>[3]</sup>试图解决部分委托问题。在该模型中, 将委托的单元进一步细化为权限, 即委托人即可以委托角色, 也可以委托权限给被委托人。PBDM 模型分为 PBDM0、PBDM1 和 PBDM2。其中, PBDM0 和 PBDM1 主要解决了用户—用户委托问题, 而 PBDM2 用来解决角色—角色委托问题。然而, PBDM2 模型与 PBDM0、PBDM1 模型之间相互独立, 因此使得 PBDM 模型不能使用一种统一的方式来处理用户—用户委托和角色—角色委托, 难于在系统中实现。

## 3 基于代理机制的访问控制模型

### 3.1 基于代理机制的访问控制模型框架

DBAC 模型的特点是引入了代理机制<sup>[4, 5, 6]</sup>来实现用户和角色之间的继承关系。它引入了对象及其代理对象的概念, 并用对象及其代理对象模拟信息系统中用户。代理机制是一种允许在类层次和实例层次上实现的继承, 而传统的 IS-A 继承是在类层次上实现继承, 委托继承则是在实例层次上实现继承。

在 DBAC 模型中, 用户被分为两类, 源用户和代理用户。信息系统中的安全管理员和高级用户被定义为源用户, 低级用户被定义为代理用户。代理用户是源用户的变换, 可部分或完全继承源用户中的权限。一个源用户可以产生一个或多个代理用户, 一个代理用户可以是多个源用户的代理用户。代理用户可以继续产生他的代理用户。代理用户中继承的权限实际上是通过切换操作调用源用户中的

权限,即读操作是读源用户的去权限,写操作则是修改源用户中的权限等。如果在权限上没有定义切换操作,那么这些权限不能被代理用户所继承。DBAC 模型框架如图 1 所示。

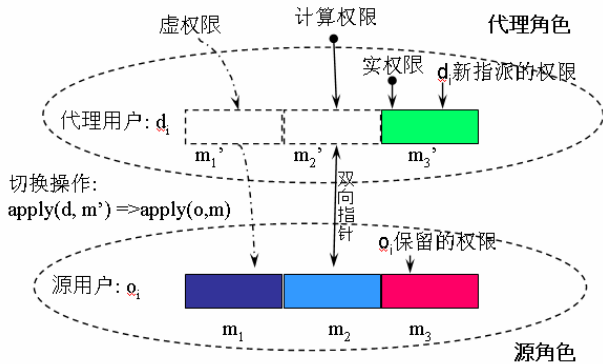


图1 基于代理机制的访问控制模型框架

如图 1 所示,源用户  $o_i$  的集合构成源角色,代理用户  $d_i$  的集合形成代理角色。源用户  $o_i$  中有三种实权限:  $m_1$ 、 $m_2$  和  $m_3$ 。代理用户  $d_i$  中有两个虚权限:  $m_1'$ 、 $m_2'$  和一个实权限  $m_3'$ 。实权限是指非继承得到的权限,虚权限则从实权限继承而来的权限,是实权限的视图。例如,图 1 中  $m_1'$  是虚权限,通过切换操作将对权限  $m_1'$  的访问转化为对权限  $m_1$  的访问。 $m_2'$  是另一种虚权限,称为计算权限,它是对源权限  $m_2$  的变换,即  $val(m_2') = Fun(val(m_2))$ , 函数  $Fun()$  通过定义在  $m_2'$  上的切换操作来实现。实权限  $m_3'$  是代理用户新指派的权限,而源用户  $o_i$  中的权限  $m_3$  是  $o_i$  的保留权限,不允许被代理用户  $d_i$  继承。

DBAC 模型提供了用户代理代数和用户代理定义语言。用户代理代数定义了 Select, Join 和 Project 三种操作。其中 Select 和 Join 是对象级别的操作,用来生成代理用户; Project 是权限级的操作,用来控制代理用户的权限。用户代理定义语言定义了泛化、特化、聚合、分组等各种语义。根据需要选择适合的定义语言和代数操作,并结合切换操作来定义具有各种语义的源角色和代理角色。

## 3.2 基于代理机制的访问控制模型定义

### 3.2.1 术语和假设

在 DBAC 模型中,存在三种不同类型的角色:基本角色(BR)、源角色(SR)和代理角色(DR)。具有相同权限的源用户被聚合为源角色,

具有相同权限的代理用户被聚合为代理角色。代理角色由安全管理员或源角色中拥有适当权限的用户通过 Select 操作、Join 操作来创建。而基本角色是没有源角色的特殊角色,是系统初始具有的或由安全管理员创建的角色。三者之间的关系如图 2 所示。

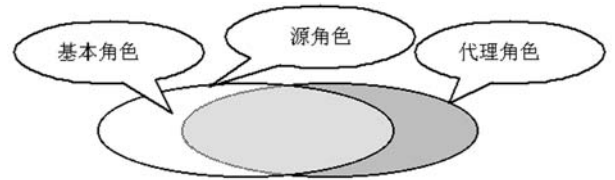


图2 三种角色之间的关系

### 3.2.2 DBAC定义

DBAC 模型的定义如下。

定义 1 DBAC 模型由以下元素组成。

1) 设 BU、SU、DU、BR、SR、DR、BP、SP、DP 分别为基本用户、源用户、代理用户、基本角色、源角色、代理角色和基本角色权限、源角色权限、代理角色权限。

2)  $U = (BU \cup DU)$ ,  $BP \supseteq (SP \cup DP)$ 。

3)  $\forall x \in DR, senior(x) \in SR$ 。

4)  $SR \subseteq (BR \cup DR)$  且  $SR \supseteq BR$ 。

5)  $SP \subseteq BP$ ;  $DP \subseteq BP$ 。

6)  $UAB \subseteq U \times BR$  为多对多的基本角色—用户指派。

7)  $UAS \subseteq U \times SR$  为多对多的源角色—用户指派。

8)  $UAD \subseteq U \times DR$  为多对多的代理角色—用户指派。

9)  $UA = UAB \cup UAD$  为多对多的角色—用户指派。

10)  $UAB \cap UAD = \emptyset$ 。

11) Role\_Can\_Deputy 关系:  $\{SR(SP), DR(DP), SC(SP, DP)\}$ 。该关系表示源角色能将其权限 SP 赋予代理角色,同时权限 SP 与代理角色中原有权限 DP 之间必须满足语义约束  $SC(SP, DP)$ 。

12) User\_Can\_Deputy 关系:  $\{SU(SP), DU(DP), SC(SP, DP)\}$ 。该关系表示源用户能将其权限 SP 赋予代理用户,同时权限 SP 与代理用户中原有权限 DP 之间必须满足语义约束

$SC(SP, DP)$ 。

### 3.3 基于代理机制的访问控制模型描述

DBAC 模型是一种灵活而强大的访问控制模型。同其他访问控制模型相比,它能用统一的模式支持多粒度代理和多步代理。

#### 3.3.1 多粒度代理

所谓多粒度代理,是指代理的单元即可以是角色,也可以是一个或多个权限。在 DBAC 中,统一通过生成源角色的代理角色的方法来实现各种粒度代理。通常使用 Select 和 Join 操作来生成代理角色。

##### (1) Select 操作定义

设  $C = \langle O^s, A^s, M^s \rangle$  为源角色,  $D = \langle O^d, A^d, M^d \rangle$  为 Select 操作生成的代理角色, 则

$$O^d = \{ o^d \mid o^d \rightarrow o^s, o^s \in O^s \wedge SC(o^s) = \text{TRUE} \}$$

其中  $o^d \rightarrow o^s$  表示  $o^s$  是  $o^d$  的源用户,  $SC(o^s) = \text{TRUE}$  表示  $o^s$  满足语义约束 SC。

##### (2) Join 操作定义

设  $C_1 = \langle O_1^s, A_1^s, M_1^s \rangle$ ,  $C_2 = \langle O_2^s, A_2^s, M_2^s \rangle$ , ...,  $C_k = \langle O_k^s, A_k^s, M_k^s \rangle$  是源角色,  $D = \langle O^d, A^d, M^d \rangle$  为 Join 操作生成的代理角色, 则

$$O^d = \{ o^d \mid o^d \rightarrow (o_1^s \times o_2^s \times \dots \times o_k^s) \in (O_1^s \times O_2^s \times \dots \times O_k^s) \wedge SC(o_1^s \times o_2^s \times \dots \times o_k^s) = \text{TRUE} \}$$

通过以上定义可知, Select 操作是从一个角色/用户中选择一个或多个权限生成代理角色/用户。Join 操作则是从几个不同角色/用户中,分别选取一个或多个不同的权限生成代理角色/用户。

#### 3.3.2 多步代理

所谓多步代理,是指一个角色/用户继承另一个角色/用户的权限后,又能将该权限向下传播。在 DBAC 中的多步代理包括角色—角色多步代理和用户—用户多步代理。

##### (1) 角色—角色多步代理

在 DBAC 中,通过生成源角色的代理角色来实现角色—角色代理。可以以一个或多个基本角色为源角色,生成基本角色的一个或多个代理角色。然后又能以这些代理角色为源角色,继续生成这些源角色的代理角色。这样就形成了一个角色链,从而自然支持多步代理。

##### (2) 用户—用户多步代理

在 DBAC 中,通过对象级别的继承操作来定义用户—用户代理,即通过以一个或多个基本用户为源用户,生成它们的代理用户。然后继续以这些代理用户为源用户,生成这些代理用户的代理用户。在这种用户—用户链中,权限可以从一个用户流动到另一个用户中。

#### 3.3.3 回收机制

在 DBAC 中,代理权限的回收也是我们要考虑的问题。代理权限可以通过三种方式回收:用户回收、安全管理员回收和系统自动回收。

##### (1) 用户回收

当用户认为不需要别人代行他的权限时,他可以从代理用户手中回收他的权限。通常的做法有以下两种:

(a) 用户直接删除代理用户的角色。这将一次性从所有代理用户中回收代理出去的权限。

(b) 用户收回某个代理用户的权限。

##### (2) 安全管理员回收

当安全管理员认为代理对象不再需要某种权限或不应再拥有某种权限时,他也可以选择回收这些角色中的权限。

##### (3) 系统自动回收

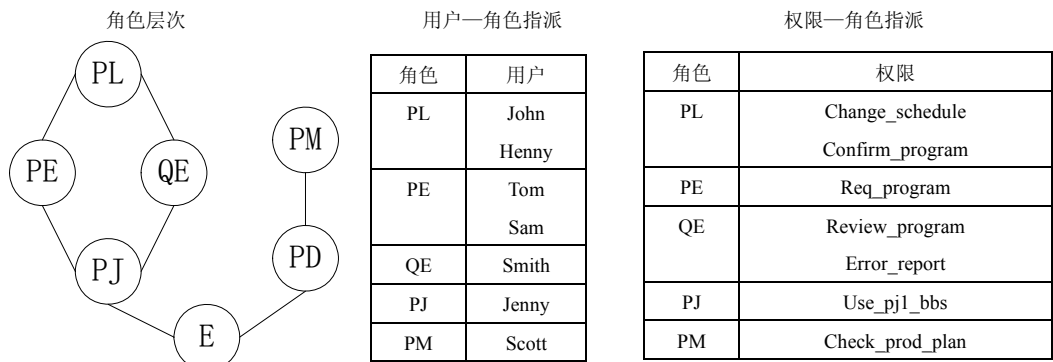
当生成代理角色或代理用户时,可以为代理类指定限制时间或限制次数属性,当代理对象的使用期达到该属性的限制时,系统将自动回收授予该代理对象的权限。

## 4 分析比较

通过如图 3 中的例子能更好地比较 DBAC 模型和 RBDM、PBDM 模型之间的差异。

由于在图 3 的情形 1 和情形 2 中,都是以权限作为传播的单位,因此,RBDM 模型无法处理这种粒度级的权限传播问题。我们主要比较 PBDM 模型和 DBAC 模型对这种场景的处理方式。

PBDM 模型使用 PBDM1 来处理情形 1(用户—用户),使用 PBDM2 来处理情形 2(角色—角色)。它们都是基于系统中某些对象(用户或角色)来创建一个临时对象(临时用户或临时角色),将这个临时对象指派给另一个对象(用户或角色)。而在 DBAC 模型中,我们通过创建源角色的代理角色,来将源角色中的权限传递给代理角色中。



情形 1: John 想让 Jenny 具有权限 “change\_schedule” 和 “PE” 角色中的权限;  
情形 2: 将角色 PL 中的权限 “change\_schedule” 赋予 “PE” 角色中的每个用户;

图 3 权限层次示例

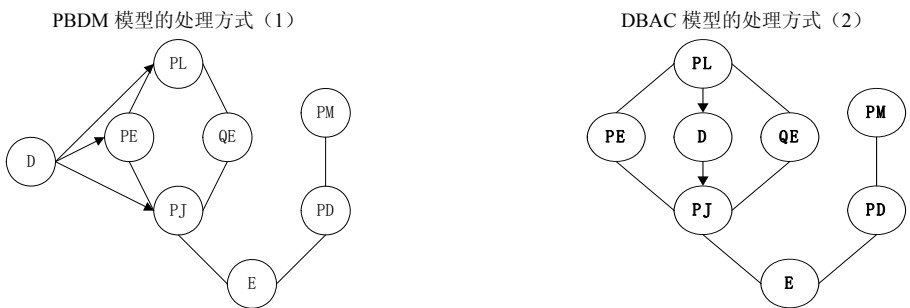


图 4 两种模型处理方式的比较

初看起来，这两种模型非常相似，基本思想都是要生成一个中间对象（用户或角色）。但这两种模型实际上是非常不同的。图 4 显示了这两种模型之间的不同。

从图 4 中，我们可以看出，在 PBDM 模型中，这种临时角色/用户与初始角色/用户和委托角色/用户之间只存在逻辑上的一一对应关系。例如，在图 4 (1) 中，临时角色 D 是基于角色 PL 创建的，它与角色 PL 相对应，但角色 PL 对临时角色 D 不存在任何约束，因此临时角色 D 可以通过角色—角色指派赋予任何角色（包括其上级角色 PL），这就产生了无效的权限流。因此在 PBDM 模型中提供三种不同的模型来处理这种情况。

在 DBAC 模型中，临时角色/用户和上级角色/用户之间具有严格的语义约束。代理角色/用户一旦创建，在角色/用户链中的位置就是固定的，因而不可能成为其上级角色/用户的源，也就避免了

无效权限流的产生。例如，在图 4 (2) 中，临时角色 D 也是基于角色 PL 创建的，但角色 PL 对临时角色 D 具有语义约束，使得 D 只可能是 PL 的下级角色，这样就保证不会产生无效的权限流。同时临时角色/用户被纳入到系统层次结构中，也便于系统管理员管理和监控。

5 结束语

DBAC 模型通过源角色/用户及其代理角色/用户之间灵活的继承关系，对访问控制提供了更加敏捷的控制方法。与其他访问控制模型相比，DBAC 使用一种统一的方法支持多粒度代理和多步代理，并支持平面角色结构和层次角色结构，因而更容易在信息系统中实现。由于 DBAC 模型本身是一种新的访问控制模型，还处于不断的发展完善过程中，还有很多其他的新特性需要进一步探索。

参考文献（略）

作者联系方式

通信地址：武汉市解放公园路 45 号网络管理中心      邮政编码：430010      联系电话：027-62740326      027-58968098

# 信息保障需求分析研究

盛丽君

**摘 要：**面对复杂多变的国际环境和互联网的广泛应用，我军信息安全问题日益突出。信息保障需求分析是构建信息保障体系的前提，如何有效地对系统进行信息保障需求分析，提高我军信息保障的能力成为了亟待解决的问题。本文对通用的分析过程和已有的分析方法进行了概述，总结了目前需求分析的不足，并结合自身特点给出了信息保障需求分析的实现方法，用以解决信息保障需求分析过程中的难点。

**关键词：**信息保障；需求分析

## 1 引言

随着信息技术的不断发展，信息安全从最初的通信安全，经历了计算机安全、信息安全，进入了信息保障阶段。各国在信息保障技术以及信息保障体系构建等方面均进行了大量的研究。但是，目前在信息保障体系构建过程中，只是参考了通用的安全体系结构，确定所需的安全防护技术，造成了系统与信息保障措施“各行其是”、保障措施并不能有效保证系统安全的问题。

因此，各国相继开始了信息保障需求分析的研究。信息保障需求分析能够使信息系统安全保障做到“应用驱动”，并通过分析其应用模式、工作过程等，确定应用系统的安全体系结构，使所有的信息保障技术措施紧密结合系统的安全需求、以满足系统安全需求为最终目的。

虽然国外对信息保障需求分析从各个角度进行了研究，但目前的信息保障需求分析理论体系和分析方法还不够完整和成熟，也没有较为统一的标准或规范。我军信息系统保障规划和建设中还缺乏对系统安全需求调研的环节。国内也相对缺乏可以应用于信息保障需求的分析方法和相应技术、工具的支撑。从总体上看，我军信息保障需求分析工作还处于起步阶段，基础薄弱，从技术研究、体系完善等方面仍与国外存在一定差距，因此，对信息安全保障需求分析的研究非常重要。

本文对国外信息保障需求分析现状进行了总结

和分析，针对我军信息保障建设初步设计了信息保障需求分析过程。

## 2 信息保障需求分析研究现状

作为信息保障技术的重要组成部分和构建基础，信息保障需求分析越来越受到人们重视。当前针对信息系统保障需求分析的研究有很多，美国国家安全局、美国国防部、加拿大安全局等部门均针对信息保障需求分析进行了研究。目前，国际上较为公认的信息保障需求分析过程指导有信息保障技术框架（IATF）和安全工程能力成熟度模型（SSE-CMM）。同时，信息保障需求分析的方法模型有基于故障树、基于用例图和基于风险评估等几类。

### 2.1 IATF及SSE-CMM中的信息保障需求分析

美国最新的信息保障技术框架（IATF）3.1 版本中增加了关于信息保障需求分析过程方面的内容，对需求分析原则、操作、结果进行了描述的进行了具体描述，并与普通的系统需求分析过程进行了对比。安全工程能力成熟度模型（SSE-CMM）则从保障步骤和保障程度两个方面进行了定义和介绍。表 1 中对应列出了，两者在通用的四个环节中定义的步骤及目标。

表 1 信息保障需求分析过程

通用环节	IATF	SSE-CMM
保障对象分析	<ul style="list-style-type: none"><li>● 分析机构的使命</li><li>● 判断信息对任务的关系和重要性</li></ul>	<ul style="list-style-type: none"><li>● 获得客户对安全需求的一种理解</li><li>● 标识该系统的目的、以便确定安全内容</li></ul>
威胁和脆弱性分析	<ul style="list-style-type: none"><li>● 确定法律和法规的要求</li><li>● 确定威胁的类别</li><li>● 判断影响</li></ul>	<ul style="list-style-type: none"><li>● 标识支配系统的法律、策略、标准、外部影响和约束</li><li>● 获得一个面向高级安全的系统操作概要获得定义该系统安全的高级目标</li></ul>
确定安全需求	<ul style="list-style-type: none"><li>● 确定安全服务</li><li>● 记录信息保护需求</li><li>● 记录安全管理角色和责任</li><li>● 标识设计约束</li></ul>	<ul style="list-style-type: none"><li>● 定义一组一致的声明，这些声明定义了该系统内部所实现的保护措施</li></ul>
评估认可	<ul style="list-style-type: none"><li>● 评估信息保护的有效性</li><li>● 向客户提供/展示文档化的信息保护需求</li><li>● 得到客户对信息保护需求的认同</li><li>● 支持系统的认证和认可（C&amp;A）</li><li>● 标识指派的批准官员（DAA）/认可员</li><li>● 标识认证专家（CA）/认证员</li><li>● 确定可适用的 C&amp;A 和采办过程</li><li>● 确保认可员和认证员对信息保护需求的认同</li></ul>	<ul style="list-style-type: none"><li>● 获得与客户需求相匹配的详细安全需求协议</li></ul>

2.2 信息保障需求分析方法

基于风险评估的需求分析方法，通常通过对保障对象的逐步细化，分析出各个组成部分的保障需求。基于故障树和用例图的需求分析方法通常以威胁分析为基础，通过对故障和误用例<sup>[1]</sup>进行逆推，得到为保护该资产所需进行的保护措施。下面

就分别对这几类分析方法进行介绍。

2.2.1 基于故障树的需求分析方法

基于故障树的信息保障需求分析方法是以软件需求为基础，采用逆推思想的信息保障需求分析方法，图 1 给出了一种较为简单的渗透故障树。

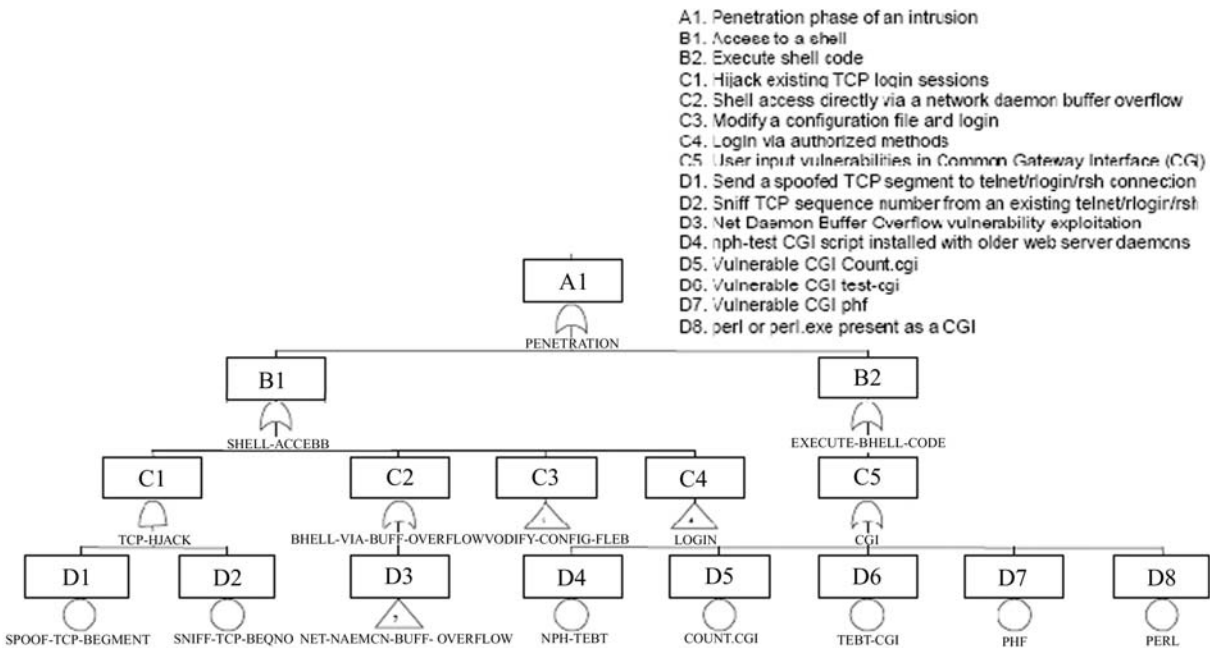


图 1 渗透故障树分析

这类方法根据系统潜在的威胁和脆弱性，逆向推导出系统可能出现故障的部分，然后根据各部分的特点分别进行保护。但这些方法不但将安全分析从系统运行环境分隔出来，而且忽略了各个组成部分相互影响关系，具有一定的局限性。

2.2.2 基于用例图的需求分析方法

为了将系统自身与外界的交流联系起来，同时照顾到各模块之间的耦合，基于不当用例的信息保障需求分析方法应运而生。文献[2]给出了一种基于UML用例图的需求分析方法，如图2所示。

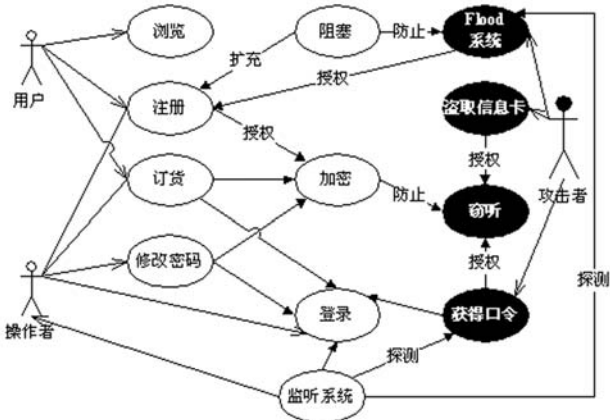


图2 不当用例关系分析

该方法从攻击者可能采取的攻击入手，通过分析不同角色对系统产生的不同影响事件，找到对系统产生威胁的不当用例，根据对不当用例进行控制措施分析得到信息保障的需求。

由于该方法从人员角色入手，而不同角色所采取的操作多种多样，所以容易产生冗余用例。

文献[3]给出了另一种事件入手的不当用例信息保障需求逆推方法，如图3所示。该方法从对系统产生威胁的事件入手，分析造成该事件所利用的系统或者管理漏洞，然后针对各个漏洞进行相应的需求措施分析。这种方法减弱了人员角色的概念，通过安全事件的产生来反映各角色参与的过程，通过分支判断减少了需求用例的冗余。

2.2.3 基于风险评估的需求分析方法

通常，在风险评估的基础上进行信息保障需求分析的方法，首先要确定需要保护的主体，其次需要确定保护的主体程度[4, 5]。文献[5]中从威胁出发，确定保护的主体，对保护的强度、时间进行定义，但是该不能够保证确定的需要保护的主体提取完备。

文献[6]在这方面进行了进一步探讨，其分析从不同层面，将系统分为组成部分，形成各类资产视图，然后对各资产的保护措施进行细化，得到最后的信息保障需求。文献[7]在以上两种方法的基础上加入了风险分析模型，其内容及分析关系如图4所示。

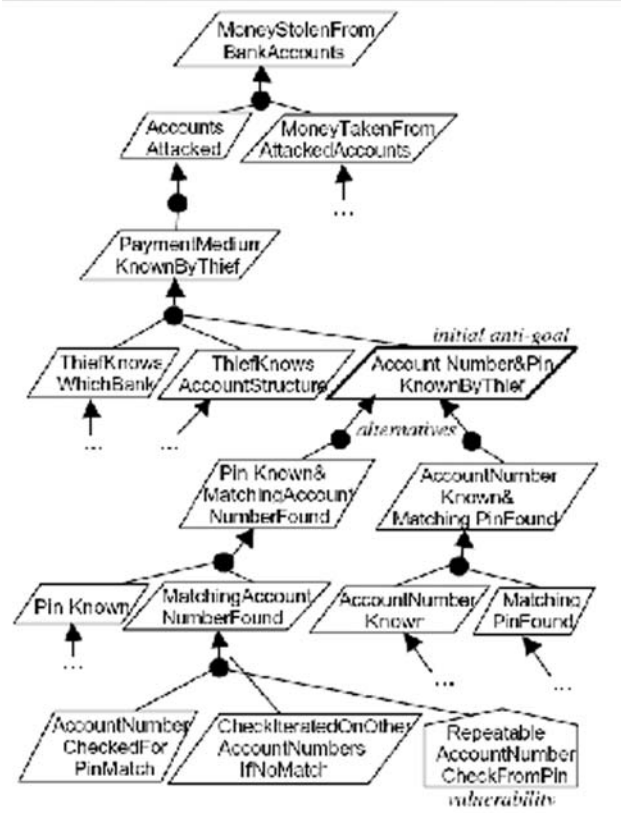


图3 基于攻击目的需求分析模型

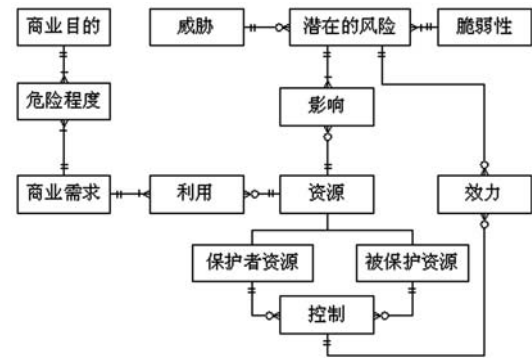


图4 安全需求分析实体关系模型

该模型在分析的过程中从商业目的出发，得出完成商业目的所需利用资源，再根据该资源的属性确定潜在的风险。在进行需求分析时，调查者加强考虑了控制手段对风险的影响。这样通过对需求分析结果对系统安全影响的强调，使需求分析结果更全面且实际操作意义更强。

### 3 信息保障需求分析过程的设计

通过以上对信息保障需求分析方法现状的研究,可以看出,信息保障分析过程是信息保障需求分析方法的基础。但是,目前关于信息保障需求分析过程的指导,主要是针对需求分析环节和目标的指导。由于调查对象及调查人员不同,实现信息保障需求分析的具体步骤细节可能有所不同。因此,我们以上述信息保障需求分析指导为基础,针对军队信息保障体系建设,初步设计了信息保障需求分析过程,主要包括以下步骤。

#### (1) 系统信息的初步采集和细化

在此之前,信息保障需求的分析者还不了解系统的应用环境和结构,所以这个环节主要的目的就是使信息保障需求的分析者能够很好的了解系统环境,并能够根据信息保障的理论将系统重新表述出来。在这个阶段,信息保证需求的分析者需要进行广泛的信息采集和沟通交互。其形式可以采取访谈类的也可以采取问卷类的,但需要尽量采取易于理解的方式,如适当减少信息保障专业概念、尽量细化问题,并根据不同角色分配问题权重等。在进行广泛的信息采集之后,需要信息保障需求的分析者进行大量的整理和转化。在此环节信息的分类和转化尤为重要,因为以后的分析将主要取决于这个时候对系统环境的形式化描述。因此,我们将被调查的对象分为:系统规划者,系统设计者,系统实现者,系统使用者等几个层面。针对系统的规划者和使用者主要采取自然语言的表述方式,其中对系统的规划者主要侧重于该系统的应用背景、整体地位等方面,对系统使用者主要侧重于该系统的使用功能和使用人员组成等方面。针对系统的设计者主要采取半形式化语言的表述方式,如系统框图,数据流图等,侧重于对系统的结构,各个子网或组件之间的联系,以及应用环境等进行调查。针对系统的实现者主要采取形式化语言,如接口分类、类表等,侧重于安全技术的实现等方面。

#### (2) 系统脆弱性分析

信息保障需求的分析者需要利用信息保障及信息安全方面的知识,对系统环境中存在的隐患进行分析。在这里我们从物理和人为两个因素进行分析,分别分析系统中物理设备、网络结构、资产等可能受到的威胁和由于组织策略及人员可信性上的威胁。通过各个威胁的逐步细化,找出系统的弱

点,也就确定了那里是需要我们给予保障的地方。因此,我们首先分析系统保护的资产。作为一个系统构建的目的,系统需要保护的资产具有很高的确定性,在各个层面各个角度的人都可以理解明确。其次,以需要保护的资产为基础,推广到这些资产所存在的物理环境,如数据流通的网络拓扑,物理设备的管理人员等。最后根据不同的物理环境,给系统定义出其用于保护资产所应有的功能、指出各个功能所实现的保障目的。

#### (3) 提出对系统的保障要求

这里的保障要求主要由威胁演变而来,保障要求与威胁相对应。此环节的目的就在于对我们的系统提出一些要求,只要能够满足这些要求,那么我们的系统就可以抵抗上述分析出的威胁,这样就使我们的信息保障框架设计更具有目的性。同时,我们也考虑到有些威胁是不能避免或不能通过系统本身的功能控制的,如某些人员威胁等。所以,在这里我们也要对那些不能抵抗的威胁给出了系统之外的解决方法,如加入强化的组织保障要求等。这样就使我们的信息保障框架不局限于技术层面,而同时关注了管理层面等。

#### (4) 保障策略选取

当确定了保障要求之后,相关的技术人员就可以根据专业知识对不同的保障要求给出相应的保障策略。这些策略主要从:环境保障策略、系统保障策略、组织保障策略三个方面进行。我们将这三个方面分别与上面的保障要求相对应。首先可以确定的是系统的保障策略,即我们的系统要采取的结构、实现的功能等等。对于系统不能达到的保障要求,我们利用对系统运行环境进行强化的方式,保证系统在该环境中运行时,不会遇到或能够抵抗该保障要求对应的威胁。对于某些人员管理等问题,需要通过一些组织保障策略来强化,如信息保障培训或者教育等。

#### (5) 对分析结果校验

在该过程中,主要是应用各种评估标准,验证给出的保障策略的合理性及其与实际情况的一致性。由于该步骤的存在,使整个分析过程产生了一个回溯环节,经过若干次的循环论证和与用户的交互,使保障需求能够更为合理,并使信息保障框架的构建者能够更深入的了解用户的需求,以达到最好的设计效果。

总体看来,实现信息保障需求分析,需要不断



将用户和应用系统的需求转化到可以具体保障策略的过程中,并通过不断的反馈、回溯,对需求分析的各个阶段进行完善和补充,最终达到符合用户要求的保障等级。

## 4 小结

本文通过对已有信息保障需求分析模型的研

究,总结出目前需求分析过程中主要需要解决的问题,并针对这些问题进行分析,设计了我军信息保障需求分析实现的方法。该方法对整个需求分析过程进行的分步细化和循环迭代,用于加强信息保障需求分析的实用性及其结果在信息保障方面的有效性。

## 参考文献

- [1] McDermott J, Fox C, Using Abuse Case Model for Security Requirements Analysis, Proc. Of the 15th Annual Computer Security Applications Conf, 1998
- [2] Sindre, G, Opdahl, A.L, Eliciting Security Requirements by Misuse Cases, Technology of Object-Oriented Languages and Systems, 2000
- [3] Axel van Lamsweerde, Elaborating Security Requirements by Construction of Intentional Anti-Models, Software Engineering, 2004. ICSE 2004
- [4] Julie J.C.H. Ryan, D.Sc, Architecting Information Assurance, Performance, Computing, and Communications, IEEE International Conference on 2004
- [5] John Rushby, Security Requirements Specifications: How and What?, Symposium on Requirements Engineering for Information Security (SREIS), March 2001
- [6] Jody Heaney, Duane Hybertson, Ann Reedy, Susan Chapin, Information Assurance for Enterprise Engineering, MITRE, PLoP 2002 conference
- [7] Evan Anderson, Joobin Choobineh, An Enterprise Level Security Requirements Specification Model, Proceedings of the 38th Hawaii International Conference on System Sciences, 2005

## 作者联系方式

通信地址:北京市 142 信箱 15 分箱

邮政编码:100854

联系电话:13366063732 (张煜冲)

# 武警部队信息安全保障系统中的VPN技术应用

苏光伟 杨海滨 杨晓元

**摘 要:** 本文在分析武警部队信息网络建设现状的基础上,研究了虚拟专用网在武警部队信息安全保障系统中的应用场合,通过对比几种虚拟专用网的特点及其使用环境,确定了各种虚拟专用网的适用范围,提出了一套虚拟专用网在武警部队信息安全保障系统中的应用方案。

**关键词:** 虚拟专用网; 信息安全; 保障系统

## 1 引言

武警部队的信息网络建设已经初具规模,取得了阶段性的成果,但网络技术日新月异,网络安全中的新问题不断出现,武警部队需要综合采用多种安全防护措施来保证其信息网络的安全。本文在对武警部队信息网络建设现状调查研究的基础上,针对其信息安全的特殊需求,提出了虚拟专用网(Virtual Private Network, 以下简称为 VPN)在武警部队信息安全保障系统中的应用方案。

## 2 VPN技术的现状

VPN 是一种新型的远程网络访问技术,最近几年得到了广泛关注。VPN 是指依靠 ISP 和 NSP,在公共网络中建立专用的数据通信网络的技术。在 VPN 中,任意两个节点之间的连接,并没有传统专用网所需的端到端的物理链路,而是利用某种公共网络的资源动态组成的。

VPN 利用公共网络基础设施,通过一定的技术手段,以达到类似私有专网的数据安全传输要求。首先,VPN 是虚拟的,并不是某个单位专有的封闭线路或者是租用某个网络服务商提供的封闭线路。其次,VPN 具有专线的数据传输功能,能够像专线一样在公共网络上处理自己单位的信息<sup>[1]</sup>。

### 2.1 VPN中的关键技术

VPN 技术非常复杂,它涉及到通信、密码和现代认证等多项技术,学科交叉性强。VPN 中的关键技术主要包含隧道技术和安全技术。

#### 2.1.1 隧道技术

隧道技术是指利用一种网络协议来传输另一种网络协议,它主要利用网络隧道协议来实现这种功能。其基本过程是在源局域网与公共网络的接口处,将数据作为负载封装在一种可以在公共网络上传输的数据格式中,在目的局域网与公共网络的接口处将数据解封装,取出负载,被封装的数据包在公共网络上传递时所经过的逻辑路径被称为“隧道”。

常见的隧道协议有四种<sup>[2-3]</sup>。

##### (1) PPTP/L2TP 协议

点到点隧道协议 PPTP (Point to Point Tunneling Protocol) 由微软公司提出,被用于 Microsoft 的路由和远程访问服务,它是数据链路层上的协议。PPTP 通过 IP 协议对 PPP 协议数据进行封装,用简单的包过滤或微软域网络控制来实现访问控制。

L2TP (Layer 2 Tunneling Protocol) 协议是国际标准隧道协议。它结合了 PPTP 协议以及第二层转发 L2F (Layer 2 Forwarding) 协议的优点,能以隧道方式使 PPP 包通过各种网络协议(包括 ATM、SONET 和帧中继等)进行传输。但是,L2TP 没有任何加密措施,实际使用中更多的是和 IPSec 协议结合使用,提供隧道验证。

##### (2) MPLS 协议

多协议标签交换是 Cisco 倡导的,后被 IETF 标准化为 MPLS,它是一种第三层的 VPN 协议。MPLS VPN 使用标签来封装原始数据,以便在计算机终端之间建立 VPN。MPLS VPN 具有很高的灵活性,可以在 VPN 终端之间采用任何网络拓扑,配置灵活,方便在众多终端之间建立全互连接性,并且,连接 MPLS VPN 中的终端时没有采用

点到点隧道,这使得 MPLS VPN 的具有很高的扩展性。MPLS VPN 的主要缺点是,在连接 VPN 终端时,这些终端处必须有服务提供商提供相应的服务。MPLS 最常见的用途是创建 MPLS VPN,另外,还可以利用流量工程使 MPLS 提供第二层 VPN 服务。

### (3) IPSec 协议

IPSec 协议不是一个单独的协议,它给出了应用于 IP 层上网络数据安全的一整套体系结构。它包括网络安全协议 AH (Authentication Header) 协议和 ESP (Encapsulating Security Payload) 协议、密钥管理协议 IKE (Internet Key Exchange) 协议和用于网络验证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换,向上提供访问控制、数据源验证、数据加密等网络安全服务。其优点是定义了一套用于提供保密性和完整性服务的标准协议,可确保运行在 TCP/IP 协议上 VPN 之间的互操作性;缺点是除了包过滤外,它没有指定其他的访问控制方法,因此它最适合于构建可信局域网之间 VPN 的应用场合。

### (4) SOCKS v5 协议

SOCKS v5 协议工作在会话层,可作为建立安全强度较高的 VPN 的基础,现在被 IETF 建议作为建立 VPN 的标准。它的优点是能够非常详细地进行访问控制,在网络层可以根据源目的 IP 地址允许或拒绝访问,而在会话层控制手段更多;由于工作在会话层,所以能同低层协议如 IPV4、IPSec、PPTP、L2TP 等一起使用;用 SOCKS v5 协议的代理服务器可隐藏网络地址结构,并能为认证、加密和密钥管理提供“插件”模块,让用户自由地采用所需要的技术;SOCKS v5 协议还可根据规则过滤数据流,包括 Java Applet 和 ActiveX 控制,因而它最适合用于客户机到服务器的连接模式,应用在外部网 VPN 和远程访问 VPN 中。

#### 2.1.2 安全技术

VPN 使用的网络是不安全的,但其传输的内容可能涉及机密数据,因此 VPN 提供的安全性服务非常重要。VPN 中使用的安全技术通常由加密技术、认证技术和密钥交换与管理技术组成<sup>[4, 5]</sup>。

##### (1) 认证技术

VPN 采用了多种认证技术,这些认证技术包括两种类型:第一种是用户身份认证。公共网络中

有很多用户和设备,如何正确地辨认合法的用户和设备,使属于本单位或授权的用户与设备能互相通信,而让未授权者无法进入系统,这就是用户与设备的身份鉴别技术要解决的问题。鉴别合法用户最常用的方法有两种,一种是用户名称与密码认证方法,另一种是卡片式两端认证方法。设备认证则需要依赖于 CA 所颁发的证书,通信双方在核对证书后,如果正确,即可交换数据。第二种认证是数据完整性和合法性认证,用于检查链路上传输的数据是否是出自源端以及在传输过程中是否被篡改过。

##### (2) 加解密技术

VPN 提供保密性服务。在传输特别敏感的数据时,需要使用加密技术。在网络层中的加密标准是 IPSec,网络层加密实现的最安全方法是在主机的端到端进行。另一个选择是“隧道模式”,加密只在路由器中进行,而终端与第一跳路由之间不加密。在终端到终端的加密方案中,VPN 安全粒度达到个人终端系统的标准;而在“隧道模式”方案中,VPN 安全粒度只达到子网标准。

##### (3) 密钥交换与管理技术

VPN 中密钥的分发与管理非常重要。密钥的分发有两种方法:一种是通过手工配置;另一种采用密钥交换协议动态分发。手工配置的方法由于密钥更新困难,只适合于简单网络的情况;密钥交换协议采用软件方式动态生成密钥,适合于复杂网络的情况且密钥可快速更新,能显著提高 VPN 的安全性。目前主要的密钥交换与管理标准有 IKE (互联网密钥交换)、SKIP (互联网简单密钥管理) 和 Oakley (键决定协议)。

## 2.2 VPN 的类型

VPN 根据不同的分类标准可以分为不同的类型。按照服务类型,VPN 大致分为四类:Intranet VPN、Access VPN、Extranet VPN 和 Intracompany VPN。通常情况下 Intranet VPN 是专线 VPN<sup>[6]</sup>。

1) Intranet VPN: 是由单位总部与分支机构之间通过公共网络构建的,这是一种网络到网络以同等的方式连接起来所组成的 VPN。

2) Access VPN: 是单位远程用户或单位的小分支机构通过公共网络远程访问单位内部网络的 VPN 方式。远程用户一般是一台计算机,而不是网络,因此组成的 VPN 是一种主机到网络的拓扑结构。

3) Extranet VPN: 是不同单位间通过公共网络来构筑的 VPN。这是一种网络到网络以不对等的方式连接起来所组成的 VPN (主要在安全策略上有所不同)。

4) Intranet VPN: 是在地理位置相对集中的局域网内部, 例如同一楼层内部的局域网内通过本地局域网线路连接起来所组成的 VPN。

### 3 VPN解决方案

目前, 武警部队已经建立了较为完善的网络环境, 并且其信息安全保障系统可以保证在网络主干线上数据的安全交换。但在主干网之外, 例如一些需要传输敏感数据而信息安全防护措施不够的场合, 以及对网络数据安全有更细化要求的场合, VPN 可以作为对现有信息安全保障系统的有效补充。

#### 3.1 Intranet VPN

武警部队的驻地在地理位置上相对分散, 支队与中队之间的距离远近不一, 虽然支队与中队之间已经实现了专线连接, 但网络架设成本较大, 维护困难, 而且网络的容错性不高, 一旦专线某处遭到破坏, 将导致网络瘫痪。同时, 由于专线连接带宽受限, 支队与中队之间的网络安全措施较少, 目前依托现有网络传输的数据类型十分有限, 网络应用范围很小。

利用 VPN 的特性可以依托公共网络组建支队范围内的 Intranet VPN, 它通过使用一个专用连接的共享基础设施, 连接各驻地, 建立相对安全的专用网络连接, 给本单位各驻地间的通信连接提供安全的网络环境。

使用 Intranet VPN 的优势在于:

- 1) 在支队到各中队的网络连接中提供了保密性服务, 避免了信息在没有保护的信道上传输;
- 2) 网络带宽可以满足同时传输语音、图像和数据等应用对高质量传输的需求;
- 3) 依托公用网络, 能更快更容易地连接新的计算机终端;
- 4) 网络容错性提高, 避免了专线某处遭到破坏而导致的网络失效, 这是由使用公用网络带来的优点。

#### 3.2 Access VPN

有些小执勤点和偏远中队离支队驻地距离较远, 而且出入这些终端节点的数据量不多, 使用专线连接网络维护费用较大。

Access VPN 可以使位于上述地点的用户通过模拟、拨号、ISDN、ADSL、移动 IP 和电缆技术, 安全地连接到支队的计算机上。Access VPN 最适用于支队局域网连接小执勤点和偏远中队的情况。小执勤点的计算机终端利用当地的 ISP 提供的 VPN 服务, 可以和支队的 VPN 网关建立私有的隧道连接, 认证服务器可对用户进行验证和授权, 保证连接的安全性。

使用 Access VPN 的优势在于:

- 1) 方便地实现了安全的拨号接入, 给小执勤点和偏远中队的计算机用户提供了安全的网络环境;
- 2) 用本地拨号接入功能来取代远距离接入, 这样能显著降低远距离通信的费用;
- 3) 支队可以便捷地对需要接入网络的新用户进行调度, 网络具有较大的可扩展性。

#### 3.3 Extranet VPN

支队之间或者同一支队的不同中队之间的网络连接一般需要经过上一级的网络中心, 其网络结构属于树型拓扑结构。在某些情况下, 支队或中队之间需要共享网络信息或者实现网络互联互通, 使用现有连接方式灵活性不高, 配置复杂, 不能满足“现联即用”的需求。而且如果使用传统的专线直接连接上述单位, 需要在支队或中队的终端上安装兼容的网络设备, 网络管理与访问控制维护复杂。

Extranet VPN 为解决以上问题提供了有效的手段, Extranet VPN 是将本单位局域网延伸至友邻单位的 VPN, 其技术与 Intranet VPN 和 Access VPN 相同, 主要的不同之处是用户连接到其友邻单位网络的需求只被许可一次。Extranet 用户对于 Extranet VPN 的访问权限可以通过防火墙等手段来灵活配置与管理。

使用 Extranet VPN 的优点在于:

- 1) 能方便地部署和管理与外部网的连接;
- 2) 连接友邻单位的网络时, 可以使用与部署 Intranet VPN 和 Access VPN 相同的架构和协议, 简化网络管理;

3) 互联互通时配置灵活, 减少了对上一级网络中心的依赖。

### 3.4 Intracompany VPN

现阶段, 支队机关局域网与 Internet 物理隔绝, 基本可以保证局域网不会受到来自外部网络的攻击。但是, 对于局域网内部的计算机用户, 局域网上没有很好的防范措施, 没有使用有效的安全策略, 因而局域网内部仍然存在安全隐患。

调查表明, 很多计算机犯罪来源于组织的内部。在支队局域网内部, 片面地相信网络内部没有网络攻击和破坏是不现实的, 即使内部用户不是故意, 也有可能无意中对面域网造成破坏。因此需要在单位内部的重要部门和重要人员之间建立安全的虚拟专线网络连接, 减少内部用户故意或无意造成的破坏。在机关局域网内部, 为了提供相对安全的网络连接, 使用 Intracompany VPN 在财务、作训等部门内部, 以及重要用户之间建立 VPN, 减

少接触到敏感信息的人数, 并防止来自局域网内部的破坏。

## 4 结语

VPN 技术是一种在公共网络上实现私有网络连接的技术, 它集中了公共网络 and 传统专网的优点。VPN 技术的最终目的是为信息共享提供安全可靠的途径, 它虽然是一项网络新技术, 但是已显示出强大的生命力。

武警部队在三级网升级改造时, 可以在其信息安全保障系统中, 根据不同的具体情况, 灵活地配置使用 VPN, 以满足支队及中队两级对网络信息安全的特殊需求, 避免信息在没有安全防护措施的网络上传播, 同时达到降低网络连接成本、提高效率和增强安全性的目的。

## 参考文献

- [1] Andrew S. Tanenbaum 著.潘爱民译.计算机网络.北京:清华大学出版社, 2004
- [2] Atul Kahate 著.邱仲潘等译.密码学与网络安全.北京:清华大学出版社, 2005
- [3] 张世永.网络安全原理与应用.北京:科学出版社, 2003
- [4] Gleeson B, Lin A, Heinanen J, et al. Feb 2000.A Framework for IP Based Virtual Private Networks, RFC 2764
- [5] Vijay Bollapragada, CCIE# 1606, Mohamed Khalid, CCIE# 2435, Scott Wainner 著.袁国忠译.IPSec VPN 设计.北京:人民邮电出版社, 2006
- [6] 王达.虚拟专用网(VPN)精解.北京:清华大学出版社, 2005

## 作者联系方式

通信地址: 陕西西安武警工程学院电子技术系系办

邮政编码: 710086

联系电话: 13359237278

# 战场数据分发系统的授权模型研究

万鑫 任毅

**摘 要:** 自动数据分发系统已经在军事应用系统中扮演越来越重要的作用。与采用“拉”传输模型的系统不同,这类系统采用的是“推”传输模型。因此自动数据分发系统的访问控制机制需要做进一步的研究。本文在对民用自动数据分发系统研究的基础上,结合战场数据分发环境的特点,提出了一个战场数据分发系统的系统框架。同时,由于战场数据的特殊性,本文提出将战场数据分发系统的授权功能必须集成到安全战场数据库中,作为安全战场数据库的一个核心功能,并提出一个安全战场数据库的访问控制模式。

**关键词:** 战场信息系统; 自动数据分发; 授权; 安全

## 1 引言

自动数据分发系统已经在当前的信息社会中发挥越来越重要的作用。这类系统根据用户事先定义的需求,自动地将满足数据用户的需求的数据传输给数据用户。战场数据分发系统作为战场信息系统的重要组成部分,无论在平时的部队训练还是战时的作战指挥中,都是不可或缺的。但正如文献[1]所指出的,这类系统的一个重要缺陷是缺乏有效的访问控制机制。因此,这类系统很少担任重要的敏感数据分发服务。对于军用系统而言,一个缺乏访问控制机制的系统是不可用的。本文在对目前商用数据分发系统的基础上,结合战场数据的特点,探讨战场数据分发系统的授权模型。

系统以用户为中心,所发送的数据依赖与特定用户的兴趣,即,用户决定他能获得什么样的数据。而战场数据分发系统以信息为中心,用户能得到什么样数据是根据当时的环境,由用户和数据管理者共同决定。这是由于军用数据的机密性要求远远超过了传统的数据分发系统的机密性要求。

此外,对于信息化条件下的现代战争而言,数据不足和数据过量都会引起灾难性的后果。因此,战场数据分发系统的数据分发策略要满足两个基本要求:① 传递给用户的信息是足够的;② 用户接受到的信息是不过量的。前者要求战场用户感兴趣的数据应该尽可能的传递给这些战场用户;后者要求随着用户特性的变化,如位置,任务变化等等,应该将一些战场用户感兴趣的数据屏蔽或缓发。要满足这两种看似矛盾的要求,需要在战场数据数据库直接支持数据分发的功能。即,数据分发的授权机制更应该在数据库内部得到支持,应该作为数据库的核心功能。

## 2 战场数据分发系统的授权要求

战场数据分发系统是战场信息系统的重要组成部分。与其他军用应用系统的授权要求相比,战场数据分发系统的授权要求具有以下不同。

1) 数据分发的模式不同。传统的军用信息应用系统采用的是一种“拉”模式。即只有当用户发出数据请求后,数据库系统根据用户身份和访问控制策略,选择数据返回给用户。而战场数据分发系统采用的是一种“推”策略。数据源周期地(或当预定义的事件发生时)将数据发送给已授权用户,不需要用户显式地发出请求。

2) 数据分发的侧重点不同。传统的数据分发

## 3 战场数据分发系统的访问控制模型

在本节中,我们首先讨论战场数据分发系统的体系结构,随后我们将讨论战场数据分发数据库中的访问控制方法。

### 3.1 战场数据分发系统框架

一个战场数据分发系统的体系结构如图 1 所示。一个用户能通过订阅模块(步骤 1)与战场数

据分发系统交互。订阅模块将用户提供的信息（如用户的标识、兴趣内容等等）进行编码，并存储在数据库中（步骤 2）。数据管理员能通过审核策略定义模块（步骤 3）来声明审核策略，即系统应该

按照怎样的策略来审核用户提交的信息，并将其存储到数据库中（步骤 4）。审核策略是军用数据分发系统与民用数据分发系统的不同之处，也是我们要研究的重点问题。

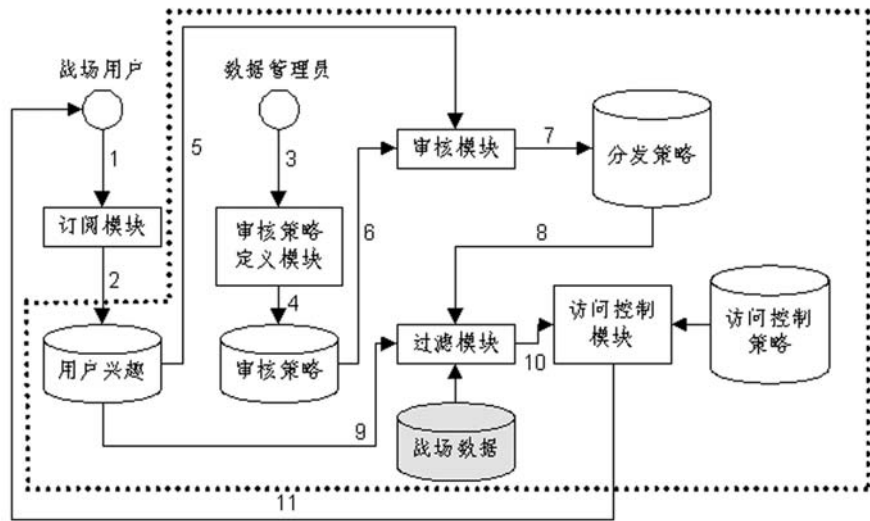


图 1 战场数据分发系统的访问控制模型框架

随后，存储在数据库中的用户兴趣和审核策略被审核模块来使用（步骤 5，6）。审核模块通过比较用户兴趣和审核策略，最终形成针对数据用户的分发策略（步骤 7）。

当战场数据分发系统获得新信息，或现存的数据信息被修改时，系统根据存储的用户兴趣和生成的分发策略，通过数据过滤模块（步骤 8，9）来准备数据。系统只选择与用户相关并满足数据分发策略的那些信息对象。过滤过程的输出是一个与用户订阅的信息的集合的子集，这是因为有一部分与用户相关的信息由于不满足对应的分发策略被过滤掉了。

在过滤阶段以后，访问控制模块被激活（步骤 10）来验证是否用户有足够的权限来访问这些被过滤模块选择的信息。访问控制模块所需要的用户数据信息已经通过过滤模块与战场数据绑定到一起。访问控制模块使用预先定义的、存储系统中的访问控制策略来做访问决策。如果用户有必要的授权，他/她将接受这些对象的一个拷贝（步骤 11）。

在图 1 中，虚线部分应该由数据库管理系统来完成。这是为了使战场敏感数据在整个系统中被最小限度的暴露。如图 1 所示，战场数据分发系统的访问控制功能由过滤模块和传统数据库的访问模块共同完成。

### 3.2 战场数据分发系统数据库访问控制框架

如上所述，战场数据分发系统的访问控制机制必须在数据库内实现，这样能保证敏感数据在最小程度上被暴露在系统以外。我们定义了一个战场数据分发系统数据库访问控制的框架，如图 2 所示。

战场数据分发系统的特点是它的用户群具有更大的异构性和动态性。在这样的场景中，授权策略所使用的传统标识机制，如基于逻辑名或用户名，将不再适用。这是因为在这种情况下，他们需要大量策略的规范说明和管理。同时在系统还应该了解用户所关注的信息类型。因此在访问控制策略的规格说明和执行中，必须包括除逻辑名以外的其他用户的特性（如用户位置、职务等）。这些属性能被视为部分标识，与用户的逻辑名等基本信息一起被编码为用户概略文件，并存储在数据库文件中。并且这些概略文件能通过证书和属性证书来验证。如图 2 所示，用户提交的信息被存储在用户概略数据表中。

在图 2 所示的分发数据库框架中，最关键的部分是审核策略元数据的定义。审核策略元数据是形成分发策略的基础，进而也是访问控制决策的基础。审核策略元数据用来定义审核策略，进一步限定用户的需求，防止用户越权要求数据，保护数据

的最小泄漏。审核策略元数据将定义如下内容。

1) 数据的用途。数据的用途表示在什么情况下用户可以使用该数据。

2) 使用者必须满足的条件。

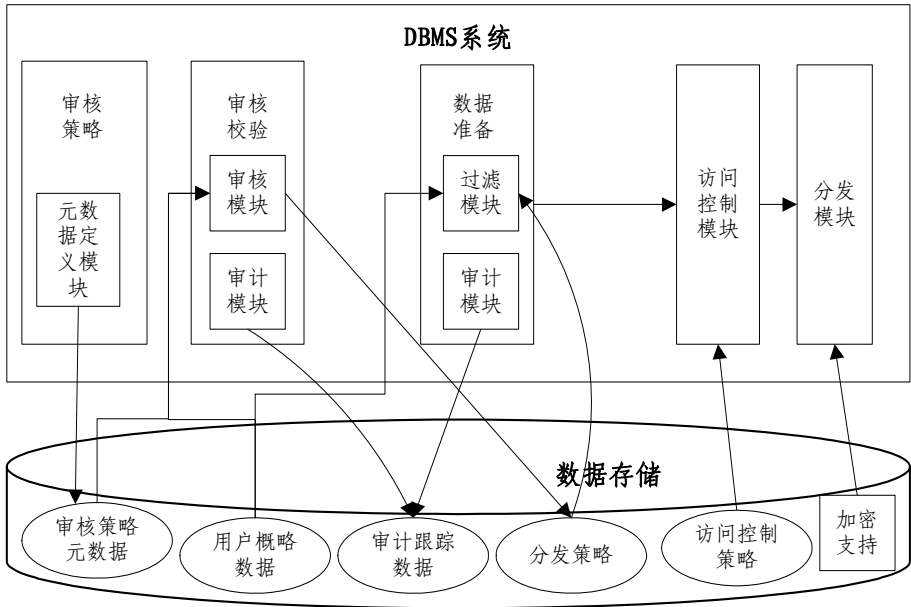


图 2 战场数据分发数据库模型框架

3) 数据的有效期。数据的有效期是指数据分发出去以后，数据用户能使用多长的时间。

我们将为每个战场数据定义相应的审核策略。这个定义过程可以在战场数据定义的过程中完成，也可以由数据管理员在事后指定。如果同一数据有不同的用途，则在审核策略元数据表中分别有多个策略来对应。同一数据不同策略所对应的分发数据也是不同的。例如，同样地形数据，分发给团级单位用来制定作战计划的精度与分发给排级单位用来指导战术行动的精度是不一样的。这种情况称为分发数据的多态性。

在数据分发系统中，为了简化管理，数据的用途被组织为一个层次结构。我们通过一个树形结构来描述数据用途之间的层次关系。树中的每个节点表示一个用途，在两个用途之间的边表示一个层次关系（如特化和泛化）。设  $U_i$ ,  $U_j$  是用途树中的两个用途。我们称  $U_j$  是  $U_i$  的一个特化（或称  $U_i$  是  $U_j$  的一个泛化），如果从  $U_i$  到  $U_j$  之间存在一个向下的路径。这条向下的路径表示用途  $U_i$  包含用途  $U_j$ 。如果用户能使用用途为  $U_j$  的数据，那么它也能使用用途为  $U_i$  的数据。

在数据分发系统中，使用者必须满足的条件是对使用者的一种约束。它包括：使用者的地位（如军衔和职务），所处的位置等等。用户只有满足这

种约束才能获得数据。例如，一个位于 A 战术地域的军官可能在他提交的概略文件中关心与其地域不相连的 C 地域的敌军信息。如果我们定义，C 地域当前的敌军信息只能分发给 C 地域及其相邻地域的军官使用，那么系统将拒绝发送相关的信息给该军官。我们通过一阶逻辑语言来描述这个条件。

数据的用途和使用者所满足的条件一起来限定用户提交的概略文件。而数据的有效期则限定用户能使用该数据的期限。该数据将随战场数据一起发送到数据使用者手中。当战场数据在用户手中停留的时间超过数据的有效期时，该数据将从用户系统中删除。

当定义了审核策略元数据以后，审核过程能利用审核策略元数据对数据用户的资格进行校验。审核过程使用用户提供的概略文件和审核策略元数据，通过比较用户的请求用途和元数据定义的用途来生成分发策略，并将该分发策略存储在分发策略表中（如图 2 所示）。审核过程的核心是找到用户请求用途和数据用途之间的映射关系。这种映射关系需要根据实际系统的需求来定义。

过滤过程根据审核过程生成的分发策略，从战场数据库中过滤数据，并将返回的数据集送到访问控制模块中做进一步的筛选。只有满足访问控制策略的那部分数据加密后通过分发过程发送出去。



最后，当战场数据分发到用户手中的时候，仍然需要对这些数据进行控制。文献[3]提出了一种访问控制策略来控制灵巧设备（如手持终端）上数据。

## 4 总结

在本文中，我们提出了战场数据分发系统的体系结构，并在该体系结构上讨论了对战场数据的授权方法。与文献[1]中提出的分发系统相比，我们增

加了对用户请求的审核。通过审核模块，我们能过滤用户请求中一些不合理的要求，防止有过量的数据分发通过战场信道传输到战场用户中。为了达到这个目的，我们使用审核元数据来定义审核的规则。我们定义了审核元数据的组成，并分析了各组成部分的作用。同时，战场数据分发系统的绝大部分工作在战场数据库中完成，从而保证数据在最小程度上暴露在数据库以外的过程中，从而减少敏感信息的泄露。

## 参考文献

- [1] E. Bertino, E. Ferrari and E. Pitoura. "An Access Control Mechanism for Large Scale Data Dissemination Systems". RIDE-DM 2001.
- [2] Yanlei Diao, Shariq Rizvi, Michael J. Franklin. "Towards an Internet-Scale XML Dissemination Service". In Proc. of VLDB, 2004
- [3] Luc Bouganim, Cosmin Cremarencu, François Dang Ngoc, Nicolas Dieu, Philippe Puchera. "Safe Data Sharing and Data Dissemination on Smart Devices", SIGMOD 2005, Baltimore, Maryland, USA, 2005 June 14-16,

## 作者联系方式

通信地址：湖北省武汉市解放公园路 43 号通信指挥学院网络管理中心

邮政编码：430010

联系电话：027-85968097

# 基于异构平台的服务异常检测系统研究

王建伟 谢永强

**摘 要:** 首先描述了服务异常检测系统的应用需求, 然后针对传统异常检测系统的不足, 设计了基于异构平台的分布式服务异常检测系统, 详细分析了该模型系统的结构功能及特点。

**关键词:** 异构; 异常检测; 网络安全; 信息安全

## 1 引言

计算机和网络正在改变人类社会的面貌, 网络应用丰富人们的生活, 同时也给我们带来了网络安全的问题。即使在配置了齐全的安全防护设备的情况下, 运行于网络中的信息系统及设备的软硬件也可能由偶然事故(例如人为的误操作)引起故障, 致使网络服务中断, 这对于一些重要信息系统(例如银行网络系统或军事信息系统)带来不可估量的损失<sup>[1]</sup>。因此, 我们不仅需要能够保证信息系统的防护安全, 还需要能够时刻监测信息系统的运行指标及检测应用服务的运行状态。同时, 网络的异构、分布、动态和开放属性要求一种新方式对开放资源进行控制和管理<sup>[2]</sup>。文中设计的基于异构平台的分布式异常检测系统可能为这一问题带来一种解决方案。

## 2 异常检测体系结构

### 2.1 系统结构设计

文中设计的基于异构平台的服务异常检测系统在功能结构上遵循 CIDF (Common Intrusion Detection Framework) 标准, 主要由控制台子系统、智能分析子系统及分布在异构网络中信息获取子系统三部分构成。信息获取子系统由 Window 代理和 linux 代理<sup>[4][5]</sup>组成, 能够不断获取所在服务器的系统工作指标, 并对服务器关键硬件参数和业务软件进行监控, 上报智能分析子系统; 智能分析子系统基于 Linux Fedora Core 2 平台实现, 是服务异常检测系统的核心, 由数据路由模块和异常检测模块等模块构成。路由模块负责转发系统内部通信, 异常检测模块负责对原始审计数据进行异常检测分析, 发现异常后向响应控制中心报告。控制台子系

统<sup>[3]</sup>为人机交互控制平台, 在控制台子系统界面可以对系统的策略配置进行更改。基于异构平台的服务异常检测系统框架结构图如图 1 所示。

### 2.2 系统功能

#### 2.2.1 信息获取子系统

信息获取子系统设计获取被监测设备的状态运行信息。信息获取子系统可分为 Windows 代理和 Linux 代理, 其中 Windows 代理结构可分为核心层和可配置代理层两个部分, 核心层作为基于异常监测的核心模块, 可配置代理层包含注册表保护、文件保护、进程监控等安全监控内容和系统日志信息。Linux 代理结构可分为通信层和业务处理层两个部分, 通信层负责与分析机子系统之间的所有通信连接与数据传输工作, 业务处理层进行具体业务逻辑处理。

代理设计用来采集系统运行状态数据, 包括网络数据、系统日志和应用日志等, 并对所采集的数据进行过滤整理等操作。它由 4 类模块组成。

1) 数据通信模块。数据通信模块的主要任务是与上层分析结构建立 tcp 数据传输通道, 通道共有两路, 一路是数据通道, 一路是命令通道, 分别进行原始信息的上报和命令的应答处理。

2) 调度管理中心。调度管理中心负责对可配置模块群的配置和管理。控制台子系统下达命令被解析后, 通过调度管理中心调用具体业务代理模块的命令接口, 来完成命令。然后通过数据通信模块将处理结果返回给上级结构。

3) 可配置模块群。可配置模块群包括信息获取模块、分析报警模块、数据处理模块、系统配置模块等, 是信息获取系统的核心。

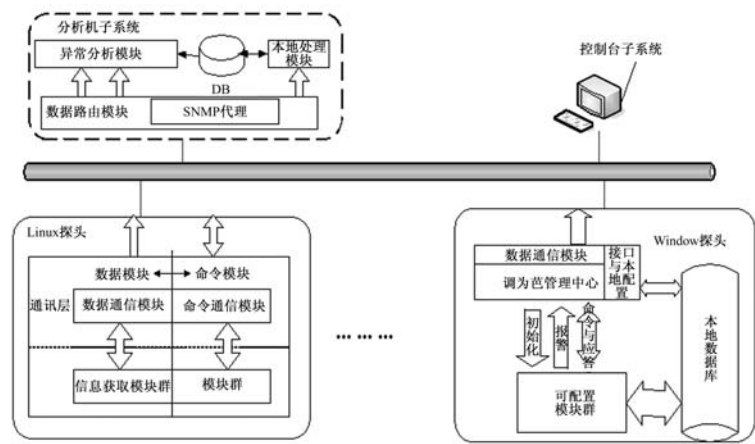


图1 系统框图

4) 本地数据库。本地数据库包括本地配置信息库和策略库，和部分业务代理模块所用到的规则库两大部分。其中本地信息库和策略库的主要作用是记录信息系统的 ip、连接端口、所加载模块等初始化配置信息，以及各模块策略配置信息等；规则库包括木马规则库、网络检测规则库、进程防火墙规则库等。这些信息库、策略库和规则库只是一个副本，是由基础平台在启动时从远端数据库中拷贝下来；每次系统启动都会和远端数据库中的主本进行版本比较，若版本较低，立即进行更新。

2.2.2 智能分析子系统

智能分析系统采用分层结构设计，主要分为通信层和业务处理层。通信层的主要功能是负责智能分析系统与信息获取系统的通信，包括的连接认证、数据接收、数据发送、数据加/解密等；业务处理层主要负责对原始审计数据进行异常检测分析。智能分析子系统有由以下几个模块构成。

1) 数据路由模块。路由模块的作用是对整个系统的应用层数据进行路由，把数据发送到相应的目的系统或者模块。根据网络路由的概念，这个系统的数据目的地址可为异常分析模块、snmp 代理模块、本地业务处理模块和智能分析子系统这 4 个模块或系统。

2) 异常分析模块。对代理发送来的原始审计数据进行异常检测分析，同数据库中调取知识比对，进行状态异常分析。

3) 数据库模块。存储模板等信息并可根据控制台子系统的命令对异常检测数据库进行各种数据的查询和管理操作。

2.2.3 接口设计

(1) 内部接口

分布式异常检测系统内部各子系统之间的通信采用自定义的数据结构。各子系统之间的接口包括：智能分析子系统与控制台子系统子系统通信接口，智能分析子系统与信息获取子系统的通信接口。

信息获取子系统（包括 windows 代理和 Linux 代理）和控制台子系统的通信进程分别与分析机子系统的通信端口进行通信；命令进程与分析机子系统的命令端口进行通信。

所有通信数据分为两部分：包头和数据，即无论是发送还是接收，首先发送或者接收包头，然后发送或者接收数据。

文中设计的系统所有内部通信采用内部管道通信和消息，所有通信数据分为两部分：包头和数据，即无论是发送还是接收，首先发送或者接收包头，然后发送或者接收数据。整个系统包头格式相同，根据包头相关标识可以确定包头后面跟随的数据格式。系统包头格式如下：

```
typedef struct _ADS_HEADER{
    char ac_CmdNum[8]; //命令号
    char ac_DataLen[8]; //传送 Data 的长度
    char ac_AnalysisFlag[16]; //分析模块标志位
    // (代理填写)
    // ac_AnalysisFlag[0]: 代表分析方法
    // ac_AnalysisFlag[1]——ac_AnalysisFlag[16]:
    // 具体服务状态
    char ac_SrcIP[16]; //源 IP
    char ac_DstIP[16]; //目的 IP
```

```
char ac_AccessTime[20];// 信息获取时间
(代理填写)
```

```
char ac_Reseve[16];//保留
```

```
}ADS_HEADER;
```

## (2) 外部接口

外部接口主要是分析机子系统与控制台子中心的接口，这部分接口主要分为两部分：Trap 告警和查询/配置接口。

服务异常检测系统分析被监控服务器状态，如果结果为异常则发送 SNMP Trap 告警给控制台子系统，控制台子系统得到异常信息后根据响应策略对整个系统作出相应的调整。

## 3 系统特点

文中设计的基于异构平台的分布式服务异常系统为异构环境下信息系统的服务异常检测提供了一个很好的解决途径，综合分析其他异常检测系统，笔者认为本系统有如下特点。

1) 文中研究的服务异常检测系统弥补了安全检测软件在服务状态检测方面的不足。

2) 文中研究的服务异常检测系统和其他的安全检测/防护设备通过 snmp 协议统一受控制台子系

统管理，并可和防火墙、蜜罐等设备进行必要的交互，达到增强安全防护能力的目的。

3) 每个代理器都是一个单独的异常检测系统，一个代理器的崩溃，对整个异常检测系统不会构成影响。

4) 系统具有很好的可扩展性，配置管理更容易，同时也可以随时更新代理检测规则。

## 4 结束语

文中设计的异构的分布式异常检测系统是一种可行和有效的方案，具有很好的应用前景。该系统除具有上述优点外，也存在一些尚待解决问题。系统的通信的安全性有赖于 tcp/ip 协议。目前 tcp/ip 协议安全服务提供的保护措施有认证、授权和访问控制、安全审计、通过对象之间的身份认证实现的安全通信、代理机制、防否认和安全信息管理等措施。Tcp/ip 协议的安全隐患比较制约整个系统的安全性。并且服务异常检测系统针对每一种服务有不同的状态检测参数，根据这些参数系统被监控的状态来判断被监控服务是否异常。随着系统开发和应用的逐步深入，这些参数可以进一步丰富、细化。

## 参考文献

- [1] Heady R, Luger G, Maccable A. The Architecture of a Network Level Intrusion system[R].Department of Computer Science,University of New Mexico,1990.
- [2] ICSA.Intrusion Detction system Buyer's Guide [DB/OL]. <http://www.icsa.net>,2002
- [3] Bace R G.入侵检测[M].陈明奇译。北京：人民邮电出版社，2001.
- [4] 毛德操，胡希明。Linux 内核源代码情景分析.浙江大学出版社.2001
- [5] 郭迪新,章克.一种分布式代理入侵检测系统的设计；湖南工程学院学报，第 14 卷 2 期，2004.6

## 作者联系方式

通信地址：北京丰台区大成路 13 号 A00

邮政编码：100039

联系电话：010-66820269-872

# 美军信息安全防护体系建设情况

王凯 李丹 黄海斌

**摘 要：**美军非常重视信息安全防护工作，视其为关系国家安全的重大战略问题。为了争夺军事信息战略制高点，美军正积极采取各种措施加强信息安全防护，建起了比较完善的信息安全防护体系。本文讲述了美军信息系统网的发展历程和美军信息安全防护技术体系，重点讲述了美军信息安全防护的主要做法。

**关键词：**美军信息系统网组成;美军信息安全防护体系;美军信息安全防护管理体制

美军信息系统网是全球规模的网络，涵盖了军队指挥、控制、通信、计算机、情报、监视与侦察（即 C<sup>4</sup>ISR）的方方面面，是美军全球军事行动的重要支撑。为保证其信息系统网的安全，美军采取了一系列措施加强信息安全防护，形成了“自上而下，分区划片”的信息安全防护管理体制，构筑了全方位的信息安全防护体系。

## 1 美军信息系统网的发展历程

美军信息系统网的发展大体经历了三个主要阶

段，即现有的国防通信系统（DCS）、在建的国防信息基础设施（DII）和全球信息栅格（GIG）。

20 世纪 60 年代初期，美军开始建设国防通信系统，现已发展为第三代全数字、全分布、多功能交换的抗干扰保密战略网。它主要保障美国总统与国防部长、参谋长联席会议主席、情报机构以及战略部队的直接通信，并负责为固定基地和陆、海、空三军的机动部队提供中枢线路。

国防通信系统是美军的主要通信系统，其组成如图 1 所示：

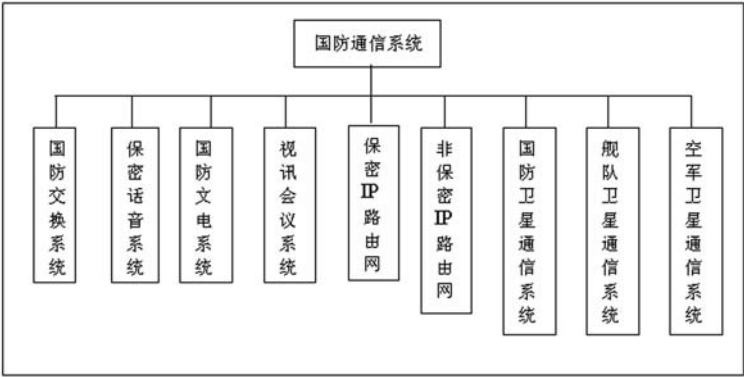


图 1 国防通信系统组成

1993 年 1 月，美国防部正式批准实施国防信息基础设施（DII）计划。该计划旨在建立一种具

有保护性能、互通和低成本的“端到端”信息传递能力。国防信息基础设施通过语音、数据、图形、图像及多媒体业务，将美国防部的任务支持系统、指挥控制系统、情报系统和用户连接在一起。

20 世纪 90 年代末，美军决定开发全球信息栅格（GIG），计划在 2010 年前初步建成。所谓 GIG，就是将保密及非密计算机网络连接成全球性

信息网，以便实现“在适当的时间以适当的格式把适当的信息传送给适当的作战人员”的设想。

## 2 美军信息网络安全防护技术体系

美军信息网络安全防护工作主要由美国国防信息系统局（DISA）负责，经过几年的建设，美军建成了如图 2 所示的信息安全防护技术体系。

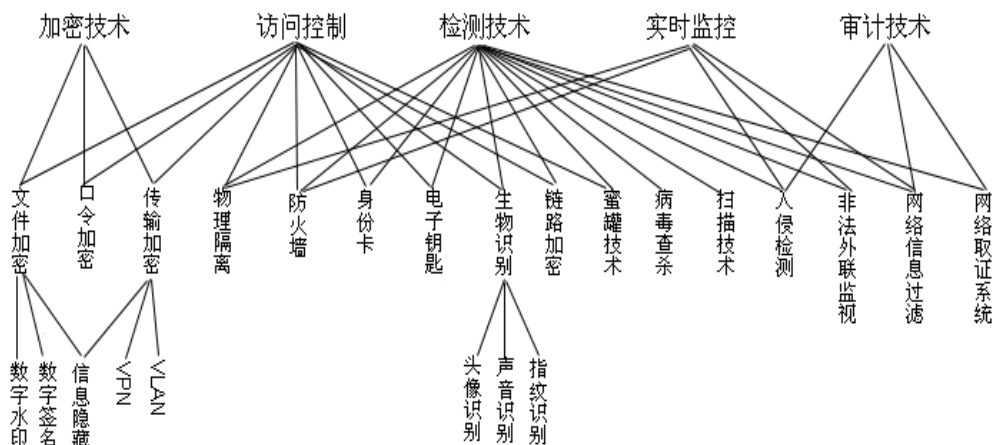


图2 美军信息安全防护体系

## 2.1 信息全程加密

文件加密器。文件加密器可保证文件的准确性和完整性，能提供识别文件源的手段，并允许在计算机之间交换加密的文件。通常，文件加密器采用图形用户界面（GUI）方式，允许用户直接选择要加密或解密的文件。

媒质加密器。媒质加密器保护数据储存媒质内容的真实性和完整性。确保配置和程序文件不被修改，媒质加密器还能在维护工作站的整体性方面起到一定作用。媒质加密器需要留出一些不加密的系统文件，以便计算机能够从硬盘驱动器引导装入程序。这些文件的大多数能够由密码检查和保护其整体性，不能防止篡改攻击，但可以警告用户数据已被更改。然而，有些系统文件包含着一些在计算机引导装入程序时更改的数据，这些文件无法受到保护。除了某些系统文件，媒质加密器对驱动器的内容都进行了加密。

口令加密。口令加密是基于密码业务供应者（CSP）的，CSP 是实际执行密码工作的独立模块。编写的 CSP 应完全独立于任何特殊的应用，这样，一个特定应用将可利用各种 CSP 来运行。实际上，某些应用可能有非常特殊的需要，因此要求定制的 CSP。CSP 能够实现整体加密算法、数字签名算法、密码散列算法、惟一标识号码、随机号码生成器、密钥存储以及只有 CSP 才有的定制设备。CSP 可用软件实现，也可用硬件实现或用二者一起来实现。

传输加密。信息在传输过程中，可以通过检测文件包的大小、状态等信息来确保其安全。状态包

过滤器不仅可以查看文件头，还能检查文件包的内容。此外，该技术能动态地保存有关过去的数据包的信息或状态信息。因此，能够根据这一状态信息制定安全策略。

## 2.2 严格访问控制

生物识别。为了确保适当的人员在适当的时间查看适合的信息，美军采用了头像识别、声音识别和指纹识别等人体生物特征来控制人员对信息的查看。

硬件标记。美军信息网系统的涉密设备，基本上都有硬件标记。国防部内一种重要的硬盘标记是 FORTEZZA 密码卡。FORTEZZA 卡为基于 FORTEZZA 的系统提供安全业务所需的密码算法。它为个人用户存储专用的密钥信息、分配认证以及加密所需的公共密钥。它执行数字签名和散列算法、公共密钥或个人专用密钥的交换功能、加密和解密。FORTEZZA 卡的接口取决于硬件平台和其配置以及操作系统。

置信计算库。可信计算系统是指能利用硬件和软件保障措施同时处理一系列敏感或保密的信息。这种系统通常要利用一个置信计算库（TCB）来实现。TCB 是在计算机系统内部的总的保护机制，包括硬件和软件，它们共同负责加强安全策略。TCB 由一个或多个部件组成，它们共同对一个产品或系统实现统一的安全策略。TCB 实现统一的安全策略的能力完全依赖于 TCB 内部的机制以及系统管理员是否正确输入有关安全策略的参数（如用户的许可证等级）。

电路网关是一种代理防火墙。电路级代理是客

户和服务器之间会话的中间连接点。客户要接入远端的服务器，首先要连到电路代理机的 TCP 端口上，然后由电路代理（在标记存取控制判决后）连接到目标服务器。存取控制是基于起始机的识别，而不翻译应用协议或审查协议包的内容。

2.3 全方位实时检测

入侵与渗透检测系统。入侵检测与反应系统可以保护网络或个人客户平台。有效的入侵检测系统可查到内部和外部的威胁。这些系统的目标是探测恶意的和无意的行动。一旦探测到入侵，一个适当的反应即被启动（如断开攻击者的连接、通知操作员、自动响应，以防止或减轻攻击、跟踪攻击之来源并记录攻击）。在传输层上工作的入侵检测机制可以审查传输包（如 TCP 包）的内容，并能够检测到比在网络层上工作的机制更复杂的攻击。工作在网络层上的入侵检测机制可以审查网络包的内容（IP 包），并只能检测网络层上出现的攻击（如端口扫描）。

病毒检测器。病毒检测器主要用来防护和查杀相关病毒，保证计算机系统及文件的安全。

3 美军信息安全防护的主要做法

3.1 信息安全防护法规明确，组织健全，领导有力

早在 1987 年，美国就颁布施行了《计算机安全法》，美军根据这部法律先后制定了一系列信息安全的法规、条例、操作规范和技术标准。其中《美军信息安全管理条例》明确提出了军事信息安全面临的主要威胁，并对军事信息安全等级进行了系统划分，详细规定了各等级军事信息安全保障的措施和法律责任，具有很强的操作性。美国国防部颁布的《网站管理指南》详细列出了国防部不宜贴于公开网站上的信息类别，包括军队作战与演习信息、个人信息、承包商提交的专利信息、可能导致不公平竞争的测试与评估信息、重大科技信息、情报信息及其他含有详细描述敏感机构动态情况的信息等。

经过多年的努力，目前，美军已形成了“自上而下，分区划片”的信息网络防护组织机构，构筑了全方位的信息安全防范管理体制，如图 3 所示。

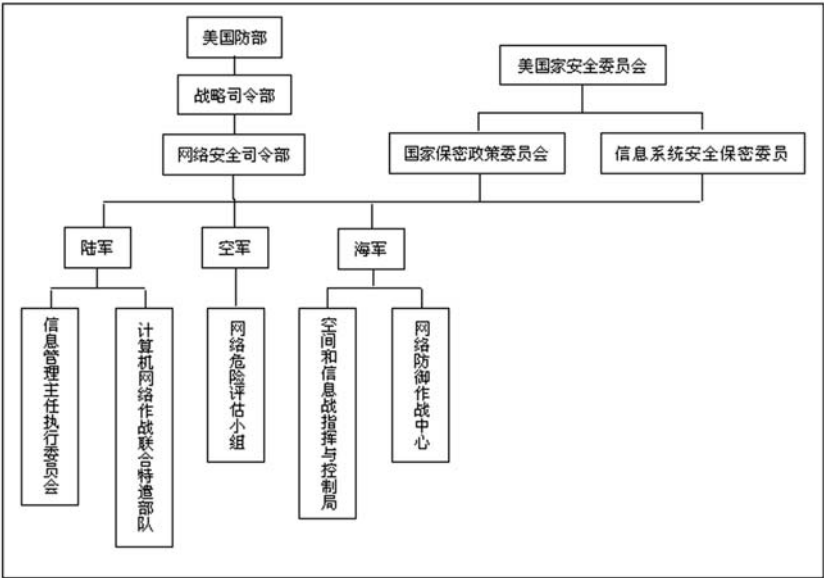


图 3 美军信息安全防护管理体制

国家保密政策委员会负责制定军事安全保密政策和数字化战场设计方案，信息系统安全保密委员会负责军事信息高速公路和数字化战场上秘密信息和敏感信息的安全保密管理。

美国防部的战略司令部，下设“网络信息安全司令部”，专门负责三军信息网络安全防护的总体

指导、规划与监督。美陆军“信息管理主任执行委员会”和“计算机网络作战联合特遣部队”，负责美军信息网络安全的监督和协调，提供网络防护预警支援。美海军“空间和信息战指挥与控制局”及“网络防御作战中心”，负责海军空间及全球远程通信保密系统的运行和维护，监控海军舰载网络、

卫星通信保密系统、海外通信保密网络与海军陆战队、海军内部网的运行，加强对海军网络系统的规范、监视和控制。美空军“网络危险评估小组”，设有互联网保密监审专员，以加强对网络的安全管理。

明确的信息安全防护法规，健全的信息安全防护组织机构，不仅使美军信息网络的安全管理与保障有了具体的负责部门，而且使各军种的网络安全防护更加统一协调，确保了美军信息系统的安全畅通。

### 3.2 信息安全防护战略指导性强，安全防护机制完善

2002年7月，美国总统布什签发《国家安全第16号总统令》规定由美国防部牵头，组织中央情报局、联邦调查局、国家安全局等部门制定出美军计算机网络战战略。该战略构想指出，在网络安全方面，美军要以最快的速度完成计算机网络防护程序与作战指挥程序的整合，建立各级司令部、各军种之间近实时的信息共享体系，评估关键系统对网络的依赖程度，尤其要监控与互联网连接网络的安全性。

“世界上没有攻不破的系统”，为及时发现系统漏洞，美军建立了信息安全风险评估机制，定期组织高级黑客对其网络进行攻击，进而对网络的保密性、完整性和可用性进行科学评价，查出网络存在的安全缺陷和漏洞并设法躲避风险。

“百思熟虑，难免一失”，为把信息安全损失降到最低，美军建立了信息安全应急反应机制，以应对随时可能发生的网络攻击。目前，美国防部和三军均参照应急作战模式分别成立了相应的网络安全防护分队。美国防部成立了“计算机网络战联合特遣部队”，专门负责处理大规模网络“入侵”事件。美陆军在欧洲和太平洋战区成立了网络应急响应部队，其主要任务是对付战术层次网络，特别是自动化指挥控制系统面临的威胁。美海军网络应急响应部队研制的自动安全事故监测系统，能全面提高网络监控能力，可识别未经授权的入网活动，自动发出警报。美空军早在1996年就建立了美军首支网络应急响应部队，目前正在研发一种自动化管理系统，以掌握空军计算机网络的被访情况，及时发现非法入侵并采取相应的安全防护措施。

### 3.3 加强人才培养，重点开发信息安全防护设备

美军认为，在未来战争中，信息网络的安全防护比保持制空权、制海权更为重要。所以，美军把信息安全人才纳入培养重点，着力建设相应的网络部队来争锋信息网络战场。在人才建设方面，美军在加强官兵的学历教育的同时，还十分注重在本国范围内聚积信息安全方面有特长的人才，并建立人才自然信息、专业信息和任务信息等人力资源数据库，在遇到战争或突发信息安全事件时可随时调用。此外，美国防大学正式成立了信息安全战略学校，专门培养高素质的安全人才，以满足不断增长的信息安全需求。

信息技术的快速发展使得信息安全产品越来越容易受到“黑客”攻击，只有加速开发并不断更新信息安全设备，才能确保信息系统的安全。为此，美军非常重视信息安全设备的研制与开发，并投入数百亿美元研制开发了密码设备、网络攻击告警系统、网络攻击智能嗅探系统和网络诱骗系统等一系列信息安全设备。

安全保密设备。美军方积极资助生物学加密技术的研究，以开发基于生物计算机的新型密码设备。美国防部正在为“全球定位系统”卫星研制一种新型军用密码（M码），以改善信号处理技术，增强保密和抗干扰能力。美国国家安全局已对美军新一代“保密终端设备”进行了认证，同意将它用于从秘密信息到绝密信息的各个领域，其加密速率达到2.4~128Kbit/s，保密呼叫仅需2秒。

网络攻击告警系统。该系统包括“深查威胁管理系统”和“深查告警服务系统”两个子系统。

“深查管理系统”可从全球180多个国家的19000多家公司的防火墙和入侵检测系统中收集攻击数据，然后向美国防信息系统局提供最新的安全信息，并定期进行情况更新。“深查告警服务系统”可收集全球1600多家信息产品供应商和3200多种信息产品在安全性方面的弱点，并通过电子邮件、传真以及短信息等方式为美国防信息系统局发送告警。

网络攻击智能嗅探软件系统。美国防部正在加紧研发“网络狼”（CYBERWOLF）软件，可实时收集、记录来自传感器、软件和计算机的入侵数据，自动处理、审查、提取、压缩入侵图样，并向管理员报告。它用一种单一的管理程序实时监测多



个数据源，可把误警、虚警率降至最低，大大提高系统的安全管理效率。

网络诱骗系统。它由美空军信息战实验室研制，用于检测、追踪和确认潜在的内外网络入侵者的信息防御系统。在网络管理员不知晓网络入侵的情况下，该系统会建立虚假网络，诱惑敌人攻击并浏览其中的虚假情报，同时将入侵者的行踪通知网络管理员。

### 3.4 开拓创新，不断拓宽信息安全领域

从法规建设到组织领导，从设备开发到人才培养，美军在信息网络安全建设方面投入了极大的精力、财力，建起了比较完善的信息安全防护体系。然而，美军并不满足，美军追求的是保持绝对的信息优势。这使得美军不断创新，不断拓宽信息安全防护领域。

2004 年 6 月 3 日，美国防高级研究计划局资助开发的世界上第一个量子密码通信网络在马萨诸塞州剑桥城投入运行实验寻求对付软件攻击的新系统。美国防部正在寻求一套新系统，它能够有效探测到通过网络传播的蠕虫和病毒，并在感染计算机之前将其隔离。这样，美国防部对付软件攻击的方法，将从原来的实时探测、响应后修复系统转变为在感染前即作出响应。另外，美国防部还在开发一套旨在保护军网免受软件攻击的高级网络安全系统，它具备对网络入侵进行实时追踪和分析的能力，可以在 4 秒钟以内确定“黑客”的身份，从而提前向网络安全员发出信号。

此外，美军还在开发便携式远程可编程无线电系统，用软件对无线电台进行远程编程，一旦设备落入敌手，可以立即更改程序，从而使无线电系统更加安全。

### 参考文献

- [1] 《美军全方位铸造信息安全防护新盾牌》，耿海军，外军瞭望，2007 年 3 月
- [2] 《美军信息安全发展综述》，周保太，国防，2006 年第 4 期
- [3] 《AD-A 393422》，美军，2003 年 4 月
- [4] 《美军信息安全主要做法及对我军的启示》，李丹，电子学会电子系统工程分会《第十四届学术年会论文集》

### 作者联系方式

通信地址：北京市丰台区大成路 13 号 S00

邮政编码：100039

联系电话：010-66820446      13437168622

# 外军信息保障研究建设现状及启示

王宁

**摘要：**面对复杂多变的国际环境和互联网的广泛应用，我军信息安全问题日益突出，如何有效地提高我军信息保障的能力为了亟待解决的问题。本文通过对外军信息保障情况进行研究，分析了外军信息保障建设的经验，并初步规划了我军建设信息保障体系的思路。

**关键词：**信息保障；GIG；深度防御

## 1 概述

目前，世界各国都深刻认识到信息、计算机、网络对于国防的重要性，并且投入大量资金进行信息安全的研究和实践。以美国为例，从总统令PDD63的颁布和实行，美国在原有基础上大力加强其信息系统的安全性保障；日本则强调，信息安全保障是日本综合安全保障体系的核心；《俄罗斯国家安全构想》中明确提出，保障国家安全应把保障经济安全放在第一位，而信息安全又是经济安全的中中之重等。可见这些国家对于信息安全的重视程度日益增加。

关于信息基础设施的安全，已经从最初提出的通信安全，向信息保障转化。本文首先研究了国内外信息保障的研究，并对美军信息化建设过程中的信息保障进行了重点分析，提出了对我军构建信息保障体系的启示。

## 2 信息保障的提出

关于信息资源的安全问题，已经从最初的通信安全，经历了计算机安全、信息安全，向信息保障发展，如图1所示。

目前，根据计算机空间安全的发展需求，信息基础设施的安全问题转化为信息保障问题。1999年美国国防部对信息保障的定义：确保信息和信息系统的可用性、完整性、可认证性、保密性和不可否认性的保护和防范活动[NISITSSI99]<sup>[1]</sup>。

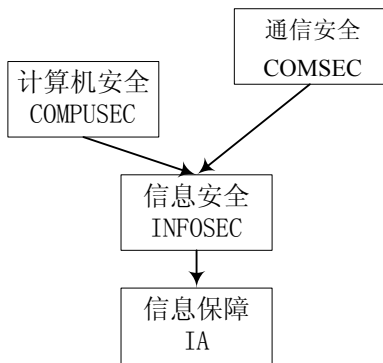


图1 信息保障（IA）的提出

我们对信息保障的理解是：信息保障是对信息和信息系统的安全属性及功能、效率进行保障的动态行为过程。它运用源于人、管理、技术等因素所形成的预警能力、保护能力、检测能力、反应能力、恢复能力和反击能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施等的机密性、完整性、可认证性、可用性、抗抵赖性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。

## 3 美军信息化建设中的信息保障情况

美军大力推进信息化建设，由于网络中心战在未来战争中发挥着重要的作用，且 GIG 是实施网络中心战的关键基础设施，美国国防部对网络中心战以及 GIG 的信息保障进行了顶层规划，并发布了相关发布的研究计划。

3.1 网络中心战中的信息保障

美军“网络中心战”已经把信息安全保障作为重点研究领域之一。为了实现网络中心战的作战思想，美军在指挥控制系统、战术互联网、数据链系统、全球网络基础设施的信息安全保障等方面开展了大量、深入研究。

美军要求其全域通信结构（含野战通信网/战术互联网）具有“纵深防御”的安全防护体系。

在全域通信系统中，提出的战术网络安全要求主要包括：

- a) 网络安全目标：为装甲车和舰艇提供全方位的通信网络安全；提供工具实现用户身份认证、阻止和检测非授权访问、全方位加密。
- b) 相关研究内容：网络中心战架构的实现，例如 JTRS；用于多级安全的通信网络的使用。
- c) 研究进度：
  - 03 年中到 04 年中，完成工具开发；
  - 04 年初到 05 年初，完成测试；
  - 04 年末到 05 年初，完成集成；
  - 05 年中，完成演示。
- d) 技术方法：使用商业产品提供无线用户身

份认证、入侵检测、访问控制，包括 PKI、数字证书、椭圆曲线加密；研究认证协议等。

3.2 GIG中的信息保障

全球信息栅格（GIG）原为国家信息基础设施（DII），在国防部的《2020 年联合构想》中改为 GIG，是网络中心战、信息优势、决策优势、全谱优势的基础和保证。GIG 是一个系统中的系统（SOS），根据作战人员、政策制定人员和支援人员的要求收集、处理、存储、分发和管理信息。GIG 一体化功能图如图 2 所示，强调提出了 GIG 应具有信息保证任务、具备信息保障能力。

由于 GIG 的重要性，它已迅速成为作战的重心。但是如果没有有效的信息保障策略，同时又面临敌军已有的信息战能力，GIG 就会恰恰成为美军的薄弱环节。对美军而言，GIG 信息保障的重要性主要体现在，如果 GIG 具有了信息保障能力，美军用户可以信任并自信地使用任何信息、实现互操作性、能够在恰当的时间访问正确的信息、获得资源保护、感知可靠的态势、安全风险的降低。因此，美军对 GIG 具有信息保障能力尤为重视，并开展了大量的研究、计划、建设。

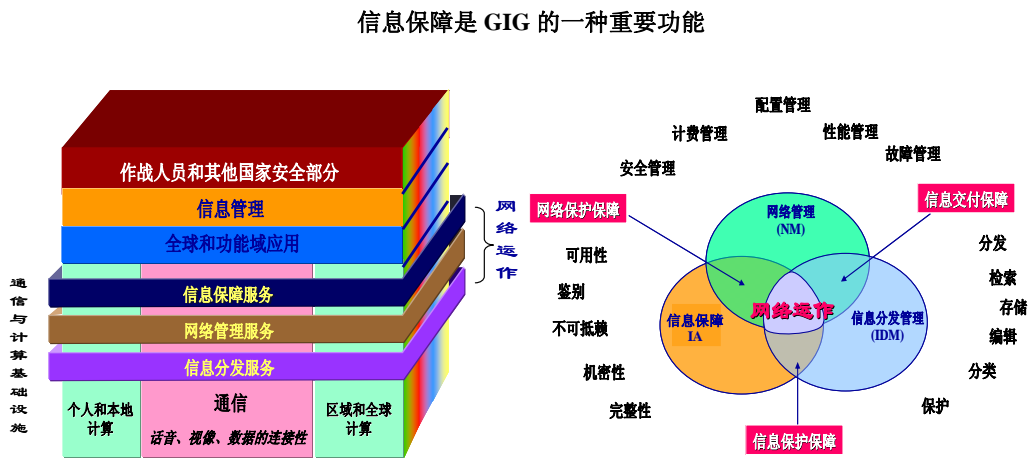


图 2 GIG 一体化功能图

- (1) 分析了 GIG 面临的威胁
- 美国防情报局（DIA）批准并发布的文件如《自动信息系统威胁环境描述（TED）》、《电子战威胁环境描述》、《对网络中心战的威胁》等文件中均对 GIG 面临的威胁进行了分析，主要包括：
- 基础设施面临威胁：美军认为，美国国家基础设施防范物理破坏、计算机攻击等的

- 能力相当脆弱，敌人可能通过远程网络、计算机终端等对 GIG 系统进行破坏。
- 面临信息战威胁：GIG 的计算机系统、操作系统和应用软件都是被攻击的目标，可能发生窃用口令与数据、注入恶意代码、拒绝服务、更改与操纵数据等攻击，导致 GIG 情报被获取并利用。

- 商用技术与商用系统带来威胁：GIG 系统采用了大量商用电子与信息技术，商用电子与信息技术的开放性、安全防护能力低给 GIG 系统带来了极大地安全威胁。

#### (2) 进行了顶层设计

美国国防部针对 GIG 的信息保障颁布了大量的 DOD 指令，规划如何实现针对 GIG 的信息保障。GIG 信息保障的目标是为 GIG 系统提供预警、保护、检测、响应和恢复功能，最终实现信息与信息系统的可用性、完整性、一致性、保密性和不可抵赖性。安全的、可信任的信息路径使作战人员能够按需访问信息，能够快速并自信地对紧急态势做出响应。

#### (3) 开展关键技术研究

为了确保运行在全球信息栅格上的各种信息系统的可靠性和安全性，防止信息的攻击与入侵，美军 DARPA 制定了一项“信息保障和可生存性”计划，其研究内容与技术主要包括：

- 研究关键基础设施的信息安全保护技术；
- 研究具有可重组、高保障、可依赖的信息保障系统；
- 研究入侵容忍系统；
- 研究故障容忍系统；
- 研究信息动态监测、管理系统等。

#### (4) 实现 GIG 信息保障的主要措施

美国国防科学委员会在《保卫美国：国防科学委员会特别小组关于防御信息战的报告，2001 年夏，第 II 卷》中指出，美国无法抵御由一个世界军事强国发起的联合性计算机网络攻击，而五角大楼正在为 GIG 开发信息安全措施。报告得出结论，五角大楼每年需要投资 30 亿美元用于计算机安全技术、训练和招募人才，以满足未来需求，这一投资数额比目前资金每年高出 14 亿美元。其中还包括在未来五年内投资 2 亿美元，用于制定相应政策，并开发出相应措施、技术、产品以保护 GIG。因此 GIG 信息保障成为了 GIG 三大组成部分<sup>[2]</sup>之一，包括信息分发管理、网络管理和信息保障，具有举足轻重的地位。

2004 年国防部发布了《DOD 信息保障战略规划框架》<sup>[3]</sup>。该框架制定了信息保障发展的国家战略计划，并分析了其信息安全技术水平和下一步发展重点。框架整体规划了 GIG 信息保障过程，确定了实施 GIG 信息保障的生命周期，制定了各阶

段的工作，并确定了 GIG 的动态信息保障的 5 个重要目标。

GIG 信息保障过程：规划、设计、实施 GIG IA 是一个不断论证的过程，首先需要针对 GIG 的特点，从信息、网络设施、态势感知、人员培训等多个方面出发确定保障目的，然后进行 GIG 信息保障的设计和实施。

#### 5 个重要目标：

- 保护信息：保证所有的信息都拥有与任务需求相适应的可信等级；
- 防御系统和网络：保证所有的访问受控、所有系统与网络具有自卫能力，要建立 GIG 网络防御体系结构、开发和执行网络安全防御政策、部署和评估网络安全防御工具、确立网络安全快速反应机制与程序、减轻内部威胁；
- 提供一体化的态势感知/信息保障指挥控制：在决策者中形成共同的理解，并生成协同行动所需的决策工具，需要开发并部署企业传感器栅格（ESG）、进行攻击指示与告警等；
- 改进并实现信息保障能力；造就一支能信息保障人才队伍。

由此可见，美军十分重视在信息战中发挥信息优势和 GIG 信息保障体系的构建。

### 3.3 信息保障技术框架

信息保障技术框架 IATF<sup>[4]</sup>是美国 NSA 的研究成果，它是不断更新、修改的，反映了 NSA 研究信息保障的阶段性成果。在 1998 年 10 月 IATF1.1 版本发布后，又发布了 IATF2.0 和 IATF3.0，目前已发布 IATF3.1。

目前 IATF 在美国得到了广泛的采纳，例如美国国防部的《全球信息栅格信息保障政策与实践指南》就是围绕深度防御战略建立，该部级的政策文档将 IATF 作为其技术解决方案的信息源和国防部信息保障实施指南。

IATF 的思想如图 3 所示。IATF 基于深度防御战略 Defense-in-Depth，就是信息保障依赖人、操作、技术三个因素实现组织的任务/业务运作。通过有效结合当前已有成熟技术，充分考虑人员、技术、操作三方面的影响，并衡量防护能力、防护性能、防护耗费、易操作性等各方面因素，得到系统

防护的最有效实用的方案。稳健的信息保障状态意味着信息保障的政策、步骤、技术与机制在整个组织的信息基础设施的所有层面上均得以有效实施。

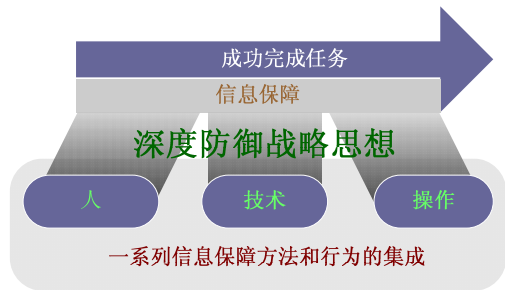


图3 深度防御思想

IATF 定义了对一个系统进行信息保障的过程，以及该系统中硬件和软件部件的安全要求。遵循这些要求和选择原则，可以对信息基础设施进行深度防御的多层防护。IATF3.1 与其之前版本相比，着重强调了信息保障需求分析的重要性，并定义了信息保障需求分析的过程。

#### 4 外军信息保障建设启示

美军随着数字化建设的推进，逐渐认识到了信息安全保障对于切实提高部队作战能力的重要性，其信息安全保障主要具有以下特点。

- 注重顶层设计：美军在进行信息系统安全防护时，注重从顶层制定信息系统安全保障计划，信息安全保障技术体现了针对防护对象分级防护、针对防护技术分层防护的思想。
- 采取多种形式防护措施：同步开发、集成多种形式的防护措施，包括对原有设备和系统进行信息安全加固，根据需求进行新技术、新工具的开发部署，设计全新的信息系统结构满足信息安全需求等。
- 目前存在的键问题：由于美军信息化建设先于信息安全建设，带来了信息安全措施目前大部分只能以“打补丁”的形式完成安全防护，美军已经认识到，这种方式不能从根本上解决信息系统存在的安全问题。

随着我军信息化进程的推进，信息保障体系建设的需求越来越迫切，开展了信息保障体系的整体

规划、关键技术的研究攻关、信息保障体系建设。但是整体上还处于建设的初步阶段，与发达国家具有一定差距。美军信息保障体系的建设对我们主要的启示：

- 重视信息保障的建设、融入信息系统建设中：美军随着部队数字化建设的推进，逐渐认识到了信息安全保障对于切实提高部队作战能力的重要性，在现有的建设部队上进行安全改进和增强。同时在 GIG 的发展建设中，美军一开始就将信息保障能力作为一项重要的能力提出，将信息保障作为 GIG 的一个子系统，使得 GIG 的信息保障能够系统、全面地实现，保证信息保障能够融入信息系统中切实发挥作用。因此我军的信息保障体系的建设也应与信息系统的建设同步进行，保证安全保障措施切实能够起到保障作用。
- 应形成信息安全保障体系：信息安全保障体系的建设不应仅仅是安全防护技术的堆叠，而应建设相应的规范体系、作战条令、作战保障等，考虑技术、人员、管理等各个方面，才能有效地发挥信息保障的作用。

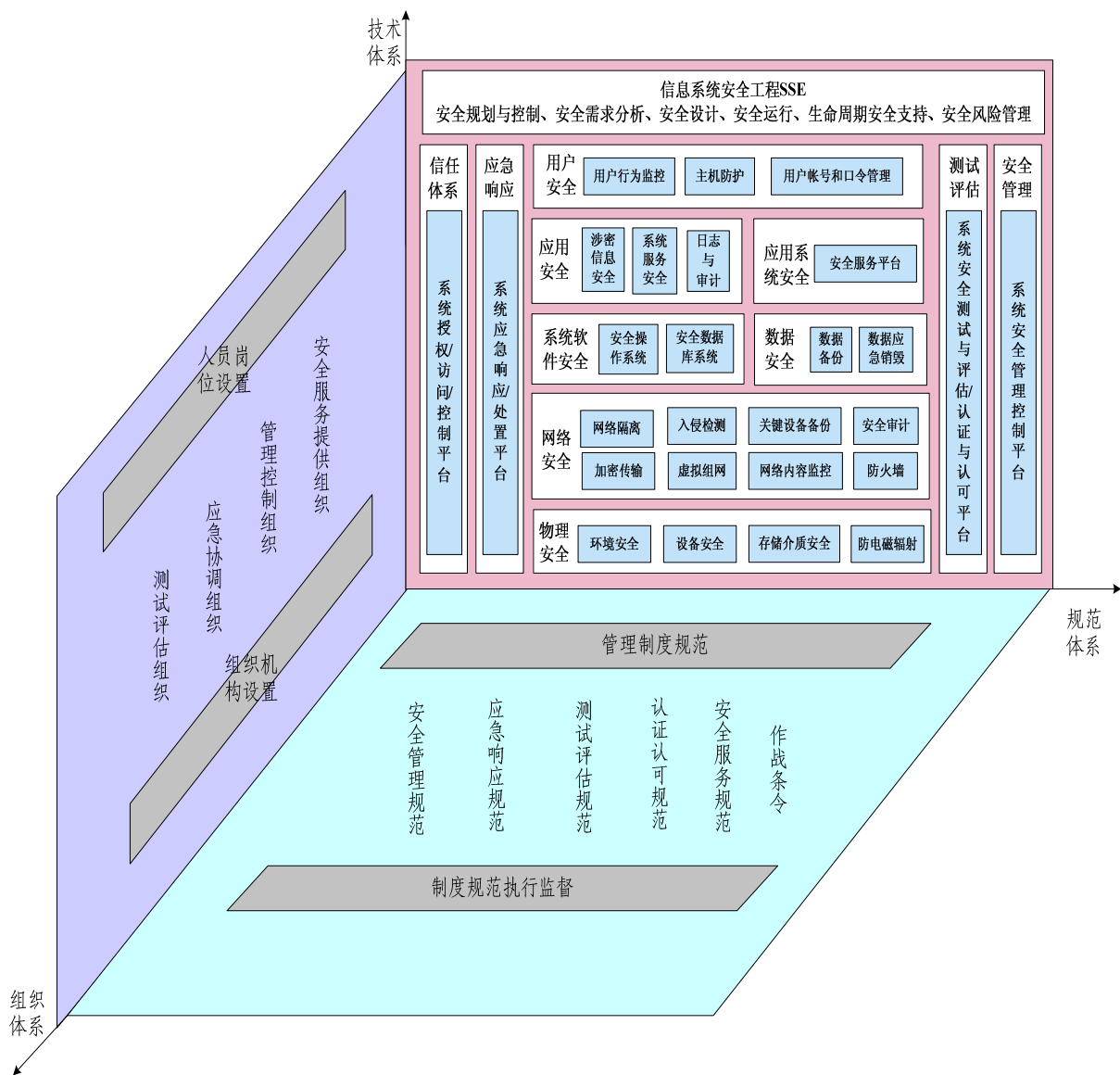
在对外军信息保障研究、建设现状分析基础上，我们提出了初步的信息保障体系规划思路，如图所示。

为了全面考虑人、操作、技术因素，从三个方面规划信息保障体系。

##### a) 技术体系

从七个方面、四个平台、一个过程建设技术体系。

- 七个方面：分别从物理安全、网络安全、系统软件安全、数据安全、应用安全、应用系统安全、用户安全建设防护体系，分别在七个方面采用相关备份、加密、审计等防护措施，实现基础保障安全。
- 四个平台：由于安全测试评估、安全管理、应急响应、信任体系是军队信息系统安全保障各个层面都需要采取的安全措施，因此分别建立平台，以解决贯穿信息保障各个防护层面的支撑技术问题。
- 一个过程：信息保障体系的建设要遵循 SSE 过程。



b) 组织体系

分别从安全管理、应急响应、测试评估、安全服务四个方面建设相应的组织结构，负责规划、执行、规范相关操作。

c) 规范体系

分别制定安全管理、应急响应、测试评估、安全服务等规范和作战条令，从而规范保障体系的建设、运行。

参考文献（略）

作者联系方式

通信地址：北京市 142 信箱 15 分箱  
邮政编码：100854  
联系电话：13366063732 （张煜冲）

5 总结

本文主要对外军信息保障理论及建设情况进行了研究，分析了外军信息保障体系建设对我军信息保障体系建设的启示，并提出了我军信息保障建设的规划思路。

# 对加强我军网络安全应急响应工作的思考

肖治庭 任毅 岳莹莹

**摘 要：**网络安全应急响应工作是我军网络安全保密工作的关键环节。为了加强我军网络安全应急响应工作，应该建立网络安全应急响应组织体系，突破网络安全应急响应手段，提高网络安全应急处置能力，重视网络安全人才培养。

**关键词：**网络；安全；应急响应

## 1 引言

网络安全应急响应是指为了应对网络安全事件的发生所做的各项准备工作，以及在安全事件发生后所采取的措施与行动。网络安全事件是指影响网络正常工作的情况，既包括主机范畴内的问题，也包括网络范畴内的问题，例如黑客入侵、病毒侵袭、信息窃取、非法信息传播、流量异常和违规操作等。采取的措施与行动主要包括对突发安全事件进行紧急处理，防止攻击的蔓延或复发，恢复正常业务，并对安全事件进行跟踪、取证，采取必要的反击措施等，其目的是避免和减小安全事件带来的影响。网络安全应急响应的指导原则是“充分准备、及时发现、快速处置、确保恢复”。为了有效地对网络安全事件进行应急响应，人们提出了网络安全应急响应六阶段方法学，即准备、确认、抑制、根除、恢复、跟踪等。

世界先进国家在网络安全应急响应方面有较为丰富的经验，早在 1988 年，美国就成立了计算机应急响应组织 CERT。目前，全球正式注册的 CERT 已达 180 多个。美国国防部和各军种也相继成立了计算机应急反应分队，能及时阻止和处理对其网络系统的攻击和破坏。2001 年 10 月，我国开始建设跨网系、跨部门、覆盖全国、网状结构的国家计算机网络安全应急响应体系，成立了国家级“互联网应急处理协调办公室”，在近年来爆发的几次大规模网络安全事件的处置中发挥了较好的作用。

当前，我军正在大力加强网络安全保密工作，因此有必要在借鉴军内外网络安全应急响应建设经验的基础上，分析我军网络安全应急响应工作现状，提出加强我军网络安全应急响应工作的对策。

## 2 我军网络安全应急响应工作现状分析

目前，我军基本建立了网络安全防护的技术防护体系、组织管理体系和法规制度体系，初步形成了具有我军特色的网络安全防护总体框架，在网络安全防护的抗毁顽存、预警监测、病毒防范、应急响应、容灾备份和密码保密等方面，都具备了一定的能力。多年来，未出现大规模病毒感染、网络攻击侵害和网络失泄密等事件，网络安全和信息保密得到可靠保证，在日常战备、作战指挥、军事训练、业务处理和部队管理等领域，发挥了显著军事效益。

但是，我们应该看到，与世界先进国家军队相比，我军网络安全应急响应工作还存在一些亟待解决的问题，主要有：

一是还没有建立起网络安全应急响应体系。我军目前还没有在各级设立专门负责协调处理网络安全突发事件的机构和岗位，各级网络执勤管理单位缺少专门的应急响应分队或人员。在预警监测、应急处置和灾难恢复等方面没有规范的管理和操作流程，还停留在经验管理阶段。

二是缺乏有效的网络安全应急处置手段。主要表现为缺乏有效的网络终端管控、安全监测和综合预警的技术手段；现有的各类安全防护技术手段间缺乏紧密关联，在安全预警、安全防护、应急响应之间还没有形成高效的闭合环。

三是网络安全应急处置能力不强。现有的各级网络安全防护人员主要侧重于关注平时有限安全事件的处理，缺乏针对战时复杂条件下网络安全应急响应的研究和训练，缺乏履行局域管控、广域监察



能力和实战经验，在遇有突发事件时，难以做出迅速、有效的应急处置。

### 3 加强我军网络安全应急响应工作对策建议

面对上述存在的问题，我们认为，应从组织体系、手段、能力和人才等四个方面加强我军网络安全应急响应工作。

#### 3.1 建立网络安全应急响应组织体系

力量建设是网络安全应急响应的根本，也是工作的重中之重。根据我军目前的编制体制，可依托已经或正在建立的各级网络安全防护中心，建立分级管理的网络安全应急响应中心，即总部、战区（含军兵种）、地区 and 用户接入网四级应急响应中心，构建军队内部纵向的网络安全应急响应体系，同时加入国家网络安全应急响应体系，建立密切的军地协作、沟通渠道，提高我军网络安全应急响应工作在早期预警、技术支持、应付突发事件等方面的能力，形成军民一体、平战结合的网络安全应急响应协作机制。各级网络安全响应中心应落实人员组成、明确人员职责分工，建立顺畅的工作指导和协作机制，根据各级网络安全状况，分类、分级制定好突发安全事件应急响应预案和处理流程，内容通常包括：应急响应组织实施、应急响应保障、应急响应处理协调、网络资源调整补充、系统参数和安全策略调整等方面的内容。

#### 3.2 突破网络安全应急响应手段

立足现有条件，紧贴作战需求，抓住“立竿见影”的关键技术环节，合力攻关、重点突破关键的网络安全应急响应手段。一是强化终端安全管控机制。对终端入网实施严格的准入控制和安全检查，对终端操作行为进行实时监控、审计和处置，从“源头”上防止黑客软件、病毒程序的攻击。二是抓紧完善网络安全监察体系。加强网络安全监察系统建设，扩大对骨干网络流量的汇聚检测范围，实现网络安全监察系统的纵向沟通；强化对网络安全防护系统配置策略的实时监测与管控，提高网络安全事件的早期预警能力，实现全军或全网范围内的安全监测数据的分析汇总、安全预警通报和安全态

势共享。三是加强网络安全防护设备“联防联控”技术研究，提高网络安全监控自动化水平，实现监控系统与防护系统的紧密联动，充分发挥现有安全资源的效能，改变多种安全防护设施“各自为战”的局面，降低安全防护系统对操作人员的依赖程度，提高安全事件及时发现和快速处置能力。四是建立容灾备份体系。依托地下防护工程，加速推进重要网络容灾备份系统建设，提高抵御灾难和重大事故的能力，确保重要网络信息系统数据和业务的持续性。五是开发基于 workflow 机制的应急处理协作响应平台，为应急响应人员提供实用的技术手段；研制相应的应急处理工具，实现对安全事件的分析、定位。

#### 3.3 提高网络安全应急处置能力

网上黑客、病毒攻击传播速度快、破坏性强、影响面广。必须采取切实有效的措施，不断提高网络安全应急处置能力和协调处理能力，确保在网络安全突发事件发生时能够准确判断、快速反应和有效应对，尽可能避免或减少网络安全突发事件对网络正常运行带来的影响和破坏。一是在梳理国内外信息战、网络战研究成果的基础上，紧密结合我军网络安全防护和应急处置实际，研究网络安全应急响应的作战指导、力量编成、组织实施、战法和训法等问题。二是在总部网络安全应急响应中心建立网络攻防实验室，通过模拟仿真、技术试验、攻击检测等方法验证网络安全应急响应理论，检验安全防护设备和系统在高强度对抗条件下的作战效能。三是制定完善各级网络安全应急响应预案，搞好有针对性的培训和演练，通过理论培训、对抗演练、联合演习等方式，提高网络安全应急响应人员在复杂条件下处置突发事件的实战能力。

#### 3.4 重视网络安全人才培养

人才是做好网络安全保密工作的关键和根本保证。网络安全保密工作的专业性、技术性很强，没有一批政治素质高、业务能力强，具备网络知识、网络安全技术、法律知识和管理能力的复合型人才和专门人才，网络安全保密就无从谈起。要把网络安全人才培养作为一项战略性工程，将网络安全人才培养纳入全军军事人才培养规划，按照满足需求、适度超前的原则，坚持军队自主培养与依托国民教育相结合，逐步形成以院校培养为主，学历教



育与短期培训、岗位历练相结合的网络安全人才培养体系。可在有关中级任职教育院校举办网络防御作战指挥培训班,培养掌握网络战理论、熟悉网络安全技术的复合型指挥参谋人才;依托有关初级任职教育院校,加强网络安全学科专业建设,培养精通网络安全技术的专业人才;采取特殊政策,特招具有特殊专长的高精尖人才,建立一支具有国际先进水平的网络安全专家队伍;采取多种方式,开展与国内著名网络安全应急响应组织在人才培养方面的交流合作,及时了解掌握国内外信息安全动态和

最新技术发展,保持人才培养的连续性和超前性。

## 4 结束语

网络安全应急响应工作是我军网络安全保密工作的关键环节。我们应该正视我军网络安全应急响应工作存在的问题,有针对性地从组织体系、手段、能力和人才等方面加强我军网络安全应急响应工作。

## 参考文献

- [1] 戴浩,我军网络安全防护急需突破的关键技术,军队指挥自动化,2006年第5期。
- [2] 庄洪林,高岩,蒋若江,军事信息系统安全保密的主要问题与对策研究,军队指挥自动化,2006年第2期。
- [3] 谢永强,加强我军信息系统安全建设的一些思考,军队指挥自动化,2006年第5期。
- [4] 武悦,对应急响应的思考,网络安全技术与应用,2006年第9期。
- [5] 钟浩,关于互联网安全应急响应的事件处理,电信科学,2006年第6期。
- [6] 段海新,计算机网络安全应急响应,电信技术,2002年第12期。
- [7] 方滨兴,建设网络应急体系,保障网络安全空间,通信学报,2002年第5期。

## 作者联系方式

通信地址:武汉市解放公园路45号网络管理中心

邮政编码:430010

联系电话:13397196993 027-85968085

# 信息隐藏技术及军事运用浅探

徐新华 黄建冲

**摘 要：**信息隐藏是近年发展起来的一种新的信息安全技术。它在数字化、网络化时代具有广阔的应用前景。文章主要阐述信息隐藏技术的历史渊源、基本概念及主要特征，并对信息隐藏的原理和模型进行了分析，最后，简单介绍了它在军事领域的主要运用。

**关键词：**信息隐藏技术；基本理论；特点；军事运用

## 1 引言

在现代战争条件下，信息对夺取战场主动权有着至关重要的作用，从工业时代起，信息技术的产生和发展始终对战争形态和作战行动方式的演变发生着重要的影响。信息隐藏技术是一门集多学科理论与技术的新兴学科。信息隐藏技术在未来战争中的应用，可以通过战场指挥、控制、通信、计算机与情报监视与侦察（C4ISR）系统利用文本、数字化的声音、图像等信息作为媒体，对作战指挥的机密信息进行隐藏传输，以防信息失密而贻误战机。因此研究信息隐藏技术在军事领域中的应用有着重要的现实意义。

## 2 信息隐藏的基本理论

### 2.1 信息隐藏技术的历史渊源及概念

现代信息隐藏技术（Information Hiding）是由古老的隐写术（Steganography）发展而来的，隐写术一词来源于希腊语，意思是将秘密信息隐藏到看上去普通的信息（如：数字图像）中进行传送的方式，其对应的英文意思是“Covered writing”。古希腊历史学家希罗多德（Herodotus, 486—425），在其著作中记录了人们首次应用隐写术的实例。现代信息隐藏技术是利用人类感觉器官对数字信号的感觉冗余，将信息隐藏在普通信息中，隐藏后信息的外部表现的只是普通信息的外部特征，不改变普通信息的本质特征和使用价值。信息隐藏技术主要运用如：高分辨率缩微胶片、扩频通信、流星余迹散射通信、语义编码（Semagram）等。其中，扩频

通信和流星余迹散射通信多用于军事上，使敌手难以检测和干扰通信信号；语义编码是指用非文字的东西来表示文字消息的内容，例如：用不同的手势可表示不同的含义；用图画、乐谱等都可以进行语义编码。

### 2.2 信息隐藏技术的原理

信息隐藏技术的模型在信息隐藏学中，通常称需要被隐藏在其他载体中的秘密信息为嵌入对象，将用于隐藏嵌入对象的公开信息称为掩护对象，嵌入对象和掩护对象可以是文本、图像或音频等等。通过使用特定的嵌入算法，可将嵌入对象添加到公开的掩护对象中，从而生成隐藏对象，这一过程称为嵌入过程。相反地，使用特定的提取算法从隐藏对象中提取出嵌入对象的过程则称为提取过程，执行嵌入过程和提取过程的个人或组织分别称为嵌入者和提取者。

在有一些特殊情况下，为了提高保密性需要预先对嵌入对象进行预处理（例如加密）生成加密信息，相应地在提取过程后也要对得到的加密信息进行后处理（例如解密），恢复原始信息。在信息隐藏系统模型的隐藏对象传输信道上存在一个隐藏分析者，隐藏分析者可对隐藏对象进行攻击，以便从中获取相关信息，一般地，攻击有被动攻击与主动攻击，对不同的信息隐藏系统其攻击的目的也不尽相同。被动攻击的主要目的有检测出隐藏对象、查明嵌入对象以及向第三方证明信息被嵌入，甚至可以指出是什么消息；主动攻击的主要目的是在不对隐藏对象做大的改动的前提下，从隐藏对象中删除嵌入对象或删除所有可能嵌入对象而不考虑掩护对象。

### 3 信息隐藏技术的特点

#### 3.1 信息隐藏技术与信息加密技术的区别

信息加密技术大家可能比较熟悉,就是利用密码学的方法,把一段明文利用一个单向函数变换为一段密文,通过公开信道送到接收方的一种技术如:保密通信,计算机密钥,防复制软盘等都属于信息加密技术。虽然信息加密技术一定程度做到了对通信双方之外的第三方隐藏其通信内容,但是使用密码方法仍有很多缺点:①加密技术主要适用于文本的加密,而对数据量很大的音频、视频、图像等多媒体数据类型往往是无能为力;②信息加密是利用物理或数学的方法将资料加密完全变为秘文,同时也暴露了消息的重要性,即使密码的强度足以使攻击者无法破解出明文,但他仍有足够的手段通过破坏通信,破坏线路等方法使得合法的接收者无法接受到信息或无法阅读信息内容;③加密技术只可以保护传输中的信息不受非法使用,无法对解密后的信息进行有效的保护。信息隐藏则不同,秘密信息被嵌入表面上看起来无害的宿主信息中例如一幅画,一段视频等,攻击者无法直观地判断他所监视的信息中是否含有秘密信息,换句话说,含有隐匿信息的宿主信息不会引起别人的注意和怀疑即使使用模式识别技术也几乎无法从中检测出是否该内容中隐藏了信息。信息隐藏的目的不是限制资料信息的交流存取,而在于保证隐藏信息不被察觉和破坏,不但隐藏了信息的内容而且隐藏了信息的存在性,这就好比隐形飞机不能被雷达探测到,从而避免了被袭击的危险。

#### 3.2 信息隐藏技术的特征

信息隐藏不同于传统的加密,因为其目的不在于限制正常的资料存取,而在于保证隐藏数据不被侵犯和发现。因此,信息隐藏技术必须考虑正常的数据操作对信息造成的威胁,即要使机密资料对正常的数据操作技术具有免疫力。对含有秘密信息的隐秘载体进行操作(如图像旋转、扭曲等几何变化、信号变换、数据压缩或者传输),不应该破坏所隐藏的秘密信息。根据信息隐藏的目的和技术要求,该技术存在以下特性。

1) 鲁棒性(Robustness):指隐藏载体对一般的信号处理(如滤波、增强、重采样、有损压缩、

D/A 和 A/D 转换等)、一般的几何变换(如平移、旋转、缩放、分割等)、恶意攻击等具有稳健性。

2) 不可感知性(Imperceptibility):指隐藏对象 S 与掩护对象 C 具有充分接近的特性。信息隐藏对人的视觉或听觉系统透明,感觉不到掩护对象的明显变化。如掩护对象与隐藏对象具有一致的噪声统计分布等,使非法拦截者无法判断是否有秘密信息存在。

3) 自恢复性:指经过了一些操作和变换后,可能会使隐藏对象受到较大的破坏,如果只留下部分的数据,在不需要宿主信号的情况下,却仍然能恢复隐藏信息的特征就是所谓的自恢复性。

4) 密钥及安全性(Security):指对密钥的保护以及嵌入算法有较强的对抗攻击能力,能够抵抗攻击者一定程度的攻击,使秘密信息不易被破坏。

5) 稳定性:指隐藏信息能“永久”的存在,并在一定的条件下可以提取。

### 4 信息隐藏主要技术

信息隐藏的主要方法包括空间域隐藏、变换域隐藏以及信道隐藏,另外还有基于文件格式和载体生成技术的隐藏。本文主要对前两种技术作简单介绍。其他的信息隐藏技术的方法也正在进一步的发展中。

#### 4.1 空域法

在空域来实现信息隐藏,多采用替换法。由于人类感觉系统的有限性,对于某些感觉变化不敏感,可直接用欲隐藏的信息来替换载体文件的数据,但不会影响到载体文件的可见性。目前比较常用的替换方法有:最不重要位替换(LSB)、伪随机置换、基于图像亮度的信息隐藏等等。最不重要位法(Least Significant Bit)是最简单的一种方法,它是通过将语音信号的部分采样值的最小权值位用代表秘密数据的二进制位替换达到将秘密信息隐藏到语音中去的目的。在接受端,只需要从相应位置提取出秘密信息比特即可。LSB 算法虽然简单易实现,信息嵌入和提取的速度快,可以隐藏的数据量大,但是其安全性很差,攻击者只需要对信道简单地加上噪声干扰或者对数据进行亚采样和压缩编码等处理都会造成整个隐秘信息的丢失。

## 4.2 变换域法

变换域法的主要特点是:利用扩频通信技术或密码学原理,将欲隐藏的信息嵌入到载体文件的变换域系数中,再经过反变换生成隐密文件(如JEPG中的隐藏算法)。它利用了人类感官系统对不同空间频率的敏感度不同来决定秘密信息嵌入位置和强度,确保嵌入信息的不可察觉性;利用图像对视觉的三个遮蔽效应:频率遮蔽、亮度遮蔽、对比度遮蔽、计算出每一块DCT的系数或每一个小波系数的可见度阈值,以此作为嵌入信号的上限强度,保证嵌入信息的不可见性。变换技术主要包括:离散傅立叶变换(DFT)、离散余弦变换(DCT)、离散小波变换(DWT)、离散哈达玛变换(DHI)、数字音频的相位编码和回声隐藏等。它与替换技术相比,隐蔽性强,健壮性较好,能抵抗噪声、压缩等攻击。

## 5 信息隐藏技术在军事上的应用

### 5.1 数据保密

在网上传输一些秘密数据要防止非授权用户截获并使用,这是军事安全的一个重要内容。我们可以通过使用信息隐藏技术来保护必须在网上交流的信息,或者对一些不愿为别人所知道的内容使用信息隐藏的方式进行隐藏存储,这样就可以不引起敌方的兴趣,从而保护了这些数据。

### 5.2 控制信息源

由于信息隐藏技术在军事领域的广泛运用,造成了一种无军事机要信息传输的假象,增加了敌方信息侦察的难度,同时有效地抵制了敌方的信息破坏。未来信息化战争,我军可从隐真与示假两方面入手,综合采取多种措施,隐蔽己方真实作战行动的同时,制造各种虚假信息,使敌方产生错觉,从而减少敌方信息侦察的正确性,误导其采取不利于敌、有利于己的决策和行动。

参考文献(略)

作者联系方式

通信地址:安徽合肥黄山路460号电子工程学院电子系407室

## 5.3 扩频通信

扩频通信可看作是一种把信息隐藏在宽频伪随机噪声中的通信方式,最典型的扩频技术为直接序列扩频和跳频扩频,它在军事中的应用可追溯到半个世纪以前。扩频通信用比发送的信息数据数率高的多的伪随机编码(掩护对象),把带信号的信息数据频谱(嵌入对象),扩展成为极低功率谱密度的宽带信号(隐藏对象)。实际上生成的隐藏对象难以和背景声(掩护对象)相区别。接收端使用相关处理方法,从收到的宽扩频信号中恢复基带信号。由于伪随机编码和信号相关处理这两大特点,使得扩频通信具有较强的抗检测性,抗干扰性和保密性。

## 5.4 攻防结合

网络为中心的战争已成为一种新的作战概念和作战样式,而且在实际中也得到了很好的应用,如美国海军提出的网络中心战战场计划,可以说在未来战争中,网络中心战将成为一种主要的作战样式。军事专家认为,堵塞或切断敌人的情报渠道最有效的措施就是对敌情报信息网络实施武力攻击或干扰。信息隐藏技术在网络战中的应用,可以通过战场C4ISR系统利用文本、数字化的声音、图像等信息作为媒体,对作战指挥的机密信息进行隐藏传输,以防信息失密而贻误战机,也可运用信息隐藏技术将各种计算机病毒、“信息炸弹”等传输到敌军的信息系统中去,在必要的时候激活它们,给敌军以致命的打击。

## 6 结束语

信息隐藏技术是一门集多学科理论与技术的新兴学科,是一种可被广泛应用在军事隐秘通信中的实用技术,已经成为现代社会中必不可少的技术之一。它与信息安全、数据加密等均有密切的关系,特别是在“制信息权”成为决定战争胜负的今天,信息隐藏技术的研究更具现实意义,我们坚信,信息隐藏技术在未来战争中必将发挥重要作用。

# DDOS攻击技术分析及其防御策略研究

许萌 贺梅 马烈

**摘 要：**网络安全中，拒绝服务攻击以其门槛低、危害巨大、难以抵御等特点成为攻击者常用的攻击手段，本文综述了 DDOS 攻击的原理及其发起攻击的体系结构，并对其防御策略进行了深入的分析研究。

**关键词：**DDOS 攻击技术；防御攻击；网络安全

## 1 引言

随着 Internet 互联网带宽的增加和各种拒绝服务工具的发布，拒绝服务攻击以其攻击范围广、隐蔽性强、简单有效等特点成为常见的网络攻击技术之一，极大影响了网络和主机系统的有效服务。全球包括 Yahoo，CNN，eBay 在内的著名网站都遭受过 DDos 攻击，使得公司损失惨重。DDos 攻击形式多样，例如黑客越来越多的利用僵尸网络（BotNet）进行分布式拒绝服务攻击，塞门铁克公司发现了一个有 40 万台主机组成的 BotNet。

## 2 DDos攻击原理及攻击体系结构

### 2.1 DDos攻击原理

DDos 是采用分布、协作的大规模攻击方式，联合或控制网络上能够发动攻击的若干主机同时发动攻击，制造数以百万计的数据流入欲攻击目标，消耗网络带宽或系统资源，致使目标主机的服务请求极度拥塞无法提供正常的网络服务。其攻击原理如图 1。

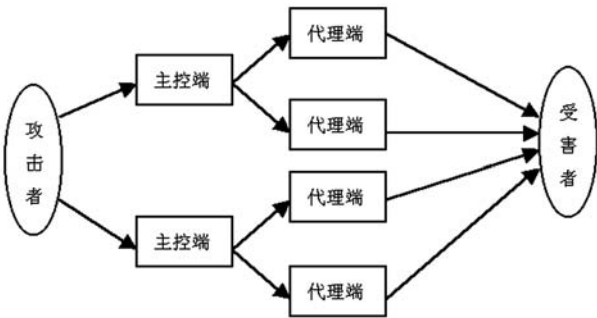


图 1 DDos 攻击原理图

DDos 攻击原理大致分为以下三种。

- 1) 通过发送大的数据包堵塞服务器带宽造成服务器线路瘫痪。
- 2) 通过发送特殊的数据包造成服务器 TCP/IP 协议模块消耗 CPU 内存资源最终瘫痪。
- 3) 通过标准的连接建立起连接后发送特殊的数据包造成服务器运行的网络服务软件耗费 CPU 内存最终瘫痪。

### 2.2 DDos攻击体系结构

DDos 攻击分为三层：攻击、主控制、代理端，三者在攻击中扮演着不同的角色。

- 1) 攻击者：攻击者所用的计算机是攻击主控制台，攻击者操纵整个攻击过程，它向主控端发送攻击命令。
  - 2) 主控端：主控端时攻击者非法侵入并控制的一些主机，这些主机黑分别控制大量的代理主机。主控端主机的上面安装了特定的程序，因此可以接受攻击者发来的特殊指令，并且可把这些命令发送到代理主机上。
  - 3) 代理端：代理端同样也是攻击者进入并控制的一批主机，它们上面运行攻击器程序，接受和运行主控端发送来的命令。代理端主机是攻击的执行者，真正向受害者主机发动攻击。
- 攻击者发动 DDos 攻击一般分为三步。第一步，寻找 Internet 上有漏洞的主机，进入系统后在其上面安装后门程序，攻击者入侵的主机越多，他的攻击队伍就越大；第二步在入侵主机上安装攻击程序，其中一部分主机充当攻击的主控制端，一部分主机充当攻击的代理端；最后各部分主机各司其职，在攻击者的调遣下对攻击对象发起攻击。

## 3 DDos攻击所用技术

### 3.1 利用软件、协议漏洞发动攻击

当受控制客户发出大量的带 SYN 标记的 TCP 请求数据包到服务器后都没有应答，使服务器端的 TCP 资源迅速枯竭，导致正常的连接不能进入，甚至致使服务器系统崩溃。

当 UDP 洪流攻击时，报文发往被攻击系统的随机或指定端口，通常是目标主机的随机端口，这使得受害系统必须对流入的数据进行分析以确定哪个应用服务请求了数据，若被攻击系统的某个攻击端口没有运行服务，它将用 ICMP 报文回应一个“目标端口不可达”消息。当控制了大量的代理主机发送这种数据包时，使得被攻击主机应接不暇，造成拒绝服务，同时也会拥塞受害主机周围的网络带宽。

ICMP 洪流攻击是通过代理向受害主机发送大量“ping”报文。这些报文涌向目标并使其回应报文，二者和起来的流量将使被攻击主机网络带宽饱和，造成拒绝服务。

### 3.2 发送异常数据包攻击

发送 IP 碎片或超过主机处理能力的数据包，致使被攻击系统主机崩溃。著名的 Teardrop 攻击就利用了某些系统 IP 协议栈中预感分片重组的程序漏洞，当数据报在不同的网络中传输时，可能需要根据网络的最大传输单元（MTU），将数据包分割成多个分片。各个网络段都有不同的能够处理的最大数据单元，当主机收到超过网络主机能够处理的网络数据包时，就无从处理这种数据报，从而引发系统崩溃。

### 3.3 对邮件系统的攻击

向一个邮件地址或邮件服务器发送大量的相同或不同的邮件，使得该地址或者服务器的存储空间塞满而不能提供正常的服务。

### 3.4 僵尸网络攻击

Bot 是 Robot（机器人）的简写，通常是指可以自动地执行预定义的功能，可以被预定义的命令控制，具有一定人工智能的程序。Bot 可以通过溢

出漏洞攻击、蠕虫邮件、网络共享、口令猜测、P2P 软件、IRC 文件传递等多种途径进入被攻击的主机，被攻击主机被植入 Bot 后，就主动和互联网上的一台或多台控制节点取得联系，进而自动接收攻击者通过这些控制节点发送的控制命令，这些被攻击主机和控制服务器就组成了 BotNet（僵尸网络）。攻击者可以控制这些“僵尸网络”集中发动对目标主机的拒绝服务攻击。

## 4 DDos攻击技术发展趋势

近几年由于宽带的普及，Windows 平台的大漏洞被公布，流氓软件、病毒、木马大量充斥着网络，一些非法攻击者可以很容易的入侵并控制大量的个人计算机来发起 DDos 攻击而从中谋利。目前 DDos 攻击从技术实现上有以下发展趋势：

- 1) 开始通过成群的受控主机进行分不是的高强度攻击；
- 2) 产生非常随机的源 IP 地址，能够更好地保护攻击源不被追踪；
- 3) 攻击数据包结构形式随机变化，很难用统一的方法检测；
- 4) 利用网络协议缺陷与系统漏洞缺陷；
- 5) 采用混合样式的攻击，加强攻击强度，增加防御难度；
- 6) 更高的发包速率，共计特征更不明显等。

## 5 防御DDos攻击的策略实施

DDos 攻击是一种相当难以防范的攻击，防御 DDos 攻击的策略需要从全局去加以部署，并且应用多种策略联动防范，将其攻击的危害降之最低，以下为几种防御 DDos 攻击的策略。

### 5.1 SYN Flood防范

SYN Flood 是一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽（CPU 满负荷或内存不足）的攻击方式。对于 SYN Flood 攻击，目前尚没有很好的监测和防御方法，但如果系统管理员熟悉攻击方法和系统架构，通过一系列的设定，也能从一定程度上降低被攻击系统的负荷，减轻负面的影响。从防御角度来说，

有几种简单的解决方法:

1) **缩短 SYN Timeout 时间**。由于 SYN Flood 攻击的效果取决于服务器上保持的 SYN 半连接数, 所以通过缩短从接收到 SYN 报文到确定这个报文无效并丢弃改连接的时间, 例如设置为 20 秒以下 (过低的 SYN Timeout 设置可能会影响客户的正常访问), 可以成倍的降低服务器的负荷。

2) **设置 SYN Cookie**。即给每一个请求连接的 IP 地址分配一个 Cookie, 如果短时间内连续受到某个 IP 的重复 SYN 报文, 就认定是受到了攻击, 以后从这个 IP 地址来的包会被丢弃。

3) **负反馈策略**。正常情况下, OS 对 TCP 连接的一些重要参数有一个常规的设置, 包括 SYN Timeout 时间、SYN-ACK 的重试次数、SYN 报文从路由器到系统再到 Winsock 的延时等。这个常规设置针对系统优化, 可以给用户提供方便快捷的服务; 一旦服务器受到攻击, SYN Half link 的数量超过系统中 TCP 活动 Half Connction 最大连接数的设置, 系统将会认为自己受到了 SYN Flood 攻击, 并将根据攻击的判断情况作出反应: 减短 SYN Timeout 时间、减少 SYN-ACK 的重试次数、自动对缓冲区中的报文进行延时等等措施, 力图将攻击危害减到最低。如果攻击继续, 超过了系统允许的最大 Half Connection 值, 系统已经不能提供正常的服务了, 为了保证系统不崩溃, 可以将任何超出最大 Half Connection 值范围的 SYN 报文随机丢弃, 保证系统的稳定性。因此, 可以事先测试或者预测该主机在峰值时期的 Half Connction 的活动数量上限, 以其作为参考设定 TCP 活动 Half Connction 最大连接数的值, 然后再以该值的倍数 (不要超过 2) 作为 TCP 最大 Half Connection 值, 这样可以通过负反馈的手段在一定程度上阻止 SYN 攻击。

4) **退让策略**。退让策略是基于 SYN Flood 攻击代码的一个缺陷。SYN Flood 程序有两种攻击方式, 基于 IP 的和基于域名的, 前者是攻击者自己进行域名解析并将 IP 地址传递给攻击程序, 后者是攻击程序自动进行域名解析, 但是两者有一点是相同的, 就是一旦攻击开始, 将不会再进行域名解析。假设一台服务器在受到 SYN Flood 攻击后迅速更换自己的 IP 地址, 攻击者不断攻击的只是一个空的 IP 地址, 并没有任何主机, 而防御方只要将 DNS 解析更改到新的 IP 地址就能在很短的时间内 (取决于 DNS 的刷新时间) 恢复用户通过域名进行的正常访问。为了迷惑攻击者, 可以放置一台

“牺牲”服务器让攻击者满足于攻击的“效果” (由于 DNS 缓冲的原因, 只要攻击者的浏览器不重起, 他访问的仍然是原先的 IP 地址)。

5) **分布式 DNS 负载均衡**。在众多的负载均衡架构中, 基于 DNS 解析的负载均衡本身就拥有对 SYN Flood 的免疫力, 基于 DNS 解析的负载均衡能将用户的请求分配到不同 IP 的服务器主机上, 攻击者攻击的永远只是其中一台服务器, 一来这样增加了攻击者的成本, 二来过多的 DNS 请求可以帮助我们追查攻击者的真正踪迹 (DNS 请求不同于 SYN 攻击, 是需要返回数据的, 所以很难进行 IP 伪装)。

6) **防火墙 Qos**。对于防火墙来说, 防御 SYN Flood 攻击的方法取决于防火墙工作的基本原理, 由于防火墙实际建立的 TCP 连接数为用户连接数的两倍 (防火墙两端都需要建立 TCP 连接), 同时又代理了所有的来自客户端的 TCP 请求和数据传送, 在系统访问量较大时, 防火墙自身的负荷会比较高, 所以这种架构并不能适用于大型网站。工作在 IP 层或 IP 层之下的称为路由型防火墙, 其工作原理有所不同: 客户机直接与服务器进行 TCP 连接, 防火墙起的是路由器的作用, 它截获所有通过的包并进行过滤, 通过过滤的包被转发给服务器, 外部的 DNS 解析也直接指向服务器, 这种防火墙的优点是效率高, 可以适应 100Mbps-1Gbps 的流量, 但是这种防火墙如果配置不当, 不仅可以让攻击者越过防火墙直接攻击内部服务器, 甚至有可能放大攻击的强度, 导致整个系统崩溃。

## 5.2 Smurf防范

1) **阻塞 Smurf 攻击的源头**。Smurf 攻击依靠攻击者的力量使用欺骗性源地址发送 echo 请求。用户可以使用路由路的访问保证内部网络中发出的所有传输信息都具有合法的源地址, 以防止这种攻击。这样可以使欺骗性分组无法找到反弹站点。

2) **阻塞 Smurf 的反弹站点**。用户可以有两种选择以阻塞 Smurf 攻击的反弹站点。第一种方法可以简单地阻塞所有入站 echo 请求, 这们可以防止这些分组到达自己的网络。如果不能阻塞所有入站 echo 请求, 用户就需要让自己的路由器把网络广播地址映射成为 LAN 广播地址。制止了这个映射过程, 自己的系统就不会再收到这些 echo 请求。

3) **阻止 Smurf 攻击平台**。为防止系统成为 smurf 攻击的平台, 要将所有路由器上 IP 的广播功

能都禁止。一般来讲，IP 广播功能并不需要。如果攻击者要成功地利用你成为攻击平台，你的路由器必须要允许信息包以不是从你的内网中产生的源地址离开网络。配置路由器，让它将不是由你的内网中生成的信息包过滤出去，这是有可能做到的。这就是所谓的网络出口过滤器功能。

4) 防止 Smurf 攻击目标站点。除非用户的 ISP 愿意提供帮助，否则用户自己很难防止 Smurf 对自己的 WAN 接线路造成的影响。虽然用户可以在自己的网络设备中阻塞这种传输，但对于防止 Smurf 吞噬所有的 WAN 带宽已经太晚了。但至少用户可以把 Smurf 的影响限制在外围设备上。通过使用动态分组过滤技术，或者使用防火墙，用户可以阻止这些分组进入自己的网络。防火墙的状态表很清楚这些攻击会话不是本地网络中发出的（状态表记录中没有最初的 echo 请求记录），因此它会像对待其他欺骗性攻击行为那样把这样信息丢弃。

### 5.3 使用DNS来跟踪匿名攻击

防范的目标并不是仅仅阻止拒绝服务攻击，而是要追究到攻击的发起原因及操作者。当网络中有人使用假冒了源地址的工具（如 tfn2k）时，虽然没有现成的工具来确认它的合法性，但可以通过使用 DNS 来对其进行分析。

假如攻击者选定了目标 `www.tttt.com`，他必须首先发送一个 DNS 请求来解析这个域名，通常那些攻击工具会自己执行这一步，调用 `gethostbyname()` 函数或者相应的应用程序接口，即在攻击事件发生前的 DNS 请求会提供给我们一个相关列表，我们可以利用它来定位攻击者。

### 5.4 主机防范

所有对因特网提供公开服务的主机都应该加以限制。下面建议的策略可以保护暴露在因特网上的主机。

- 1) 将所有公开服务器与 DMZ 隔离；
- 2) 使用 SRP (Secure Remote Password 安全远程口令) 代替 SSH；

参考文献（略）

作者联系方式

通信地址：北京北四环中路 226 号中心 61901 部队  
 邮政编码：100083  
 联系电话：010-66305573

3) 限制只有内部地址才能访问支持 SRP 的 telnet 和 FTP 守护程序；

4) 使用内置防火墙；

5) 使用一些防端口扫描措施。如使用 Linux 的后台程序功能或通过修改内核实现；

6) 使用 Tripwire 和相同作用的软件来帮助发觉对重要文件的修改。

### 5.5 电子邮件炸弹防护

保护电子信箱邮件的信息安全最有效的办法就是使用加密的签名技术，如 PGP 来验证邮件，通过验证可以保护到信息是从正确的地方发来的，而且在传送过程中不被修改。

就电子邮件炸弹而言，可以使用 `http://semxa.kstar.com/hacking/echom201.zip` E-mail Chomper（砍信机）来保护自己。但是目前就国内用户而言，大多用户所使用的都是免费的邮箱，像 `yeah.net`、`163.net`、`263.net` 等，即便是有人炸顶多也是留在邮件服务器上了，危害基本上是没有的。如果是用 pop3 接的话，可以用 Outlook 或 Foxmail 等 pop 的收信工具来接收的 mail，大多用户使用的是 windows 的 Outlook Express，可以在“工具—收信箱助理”中设置过滤。对于各种利用电子邮件而传播的 Email 蠕虫病毒和对未知的 Email 蠕虫病毒你可以使用防电子邮件病毒软件来防护。

另外，邮件系统管理员可以使用“黑名单”来过滤一些垃圾信件。对于不同的邮件系统，大都可以在网络上找到最新的黑名单程序或者列表。

## 6 小结

现在对于 DDos 攻击并没有 100%有效的防御手段，但我们应通过深入地分析，了解各种 DDos 攻击的方式，只有采取主动措施，积极部署防御策略，才能缓解和抵御此类安全威胁。



# 一种提高扩频信号隐蔽性的有效方法

严文超 赵杭生

**摘要：**数字信号处理方法的发展为研究人员提供了很多对扩频信号进行参数估计的工具，现有的很多种参数估计和扩频序列估计方法使得直接序列扩频信号的隐蔽性不复存在，本文针对功率谱二次处理法和基于矩阵分解的扩频序列估计方法，提出了直接序列扩频调制的改进方案，进一步提高了直接序列扩频信号的隐蔽性，并对其性能进行了仿真分析。

**关键词：**直接序列扩频；参数估计；隐蔽性；

## 1 引言

在无线通信中，扩频通信以其强抗干扰能力，低截获概率，良好的隐蔽性和保密性，在军事通信中得到广泛应用，是通信抗干扰的一种重要手段。

直接序列扩频通信技术将信号能量扩展到带宽很宽的频带，功率谱密度较低，具有一定的隐蔽性。对于直接序列扩频通信的侦察，一般侦察接收机要完成以下几个部分的工作：通过检测方法判断是否有直接序列扩频信号存在；对载波频率、扩频码周期和扩频码速率等扩频参数进行盲估计；根据估计到的信息配合各种解调方法进行解扩解调。

直接序列扩频信号的基本参数包括：载波频率、载波相位、伪码周期、码元宽度、码片速率、扩频序列等。对于载频的提取方法主要有平方倍频法和循环谱检测等方法<sup>[1-2]</sup>；码片速率和码元周期的提取可以分别通过延迟相乘法和功率谱二次处理法来实现<sup>[3-4]</sup>；扩频序列的估计，主要有以下两种方法：最早提出的基于矩阵分解的分析方法<sup>[5]</sup>和基于神经网络的扩频序列估计方法<sup>[6]</sup>。

Gilles Burel 等人利用基于矩阵分解的分析方法假设扩频周期已知，在-9dB 的高斯白噪声环境下，成功实现了对周期为 31 的 Gold 码序列的正确估计<sup>[5]</sup>。张天骐等人利用功率谱二次处理法在-14dB 的高斯白噪声环境下，成功实现了对长度为 100 的 PN 码的周期的估计<sup>[4]</sup>。这两种方法的结合对扩频信号的隐蔽性造成极大的威胁。

文章介绍了基于矩阵分解的扩频序列估计方法和功率谱二次处理方法的原理，并在此基础上提出一种直接序列扩频调制的改进方法，即在发送端采用符号周期不等于扩频序列周期的方式对信息进行

扩频， $T_s \neq NT_c$  ( $T_s$  为符号周期， $N$  为扩频序列长度， $T_c$  为码片周期)，在一定程度上打乱直接序列扩频信号的某些规律性，使得以上两种方法不能实现对扩频序列的估计，进一步提高扩频信号的隐蔽性。

## 2 基于矩阵分解的扩频序列估计方法

### 2.1 工作原理

假定码元周期已知、采样周期等于码片周期。将接收到的直接序列扩频信号分成长度为码元周期的许多段，记做  $\mathbf{y}$ ，由此可以估计信号的自相关矩阵  $\mathbf{R}$ 。

$$\mathbf{R} = E\{\mathbf{y} \cdot \mathbf{y}^H\} \quad (1)$$

由于同步的问题的存在，假设  $P$  为扩频码长度， $T_s$  为符号周期， $T_e$  为抽样周期， $T_c$  为码片周期 ( $T_c = T_s/P$ )， $\sigma_n^2$  为噪声方差， $\sigma_s^2$  为信号方差， $\rho = \sigma_s^2/\sigma_n^2$  为信噪比， $t_0$  为解同步时间， $\lambda_i$  ( $i=1, 2, \dots, P$ ) 为  $\mathbf{R}$  的特征值， $a_m$  为第  $m$  个信息， $\mathbf{p}_0$  为由扩频序列的后  $P(T_s - t_0)$  个码元和  $Pt_0$  个零组成的向量， $\mathbf{p}_1$  为由  $P(T_s - t_0)$  个零和扩频序列的前  $Pt_0$  个码元组成的向量， $\mathbf{n}$  为噪声。

$$\mathbf{y} = a_m \mathbf{p}_0 + a_{m+1} \mathbf{p}_1 + \mathbf{n} \quad (2)$$

式 (2) 代入式 (1) 得

$$\mathbf{R} = E\{\|\mathbf{a}_m\|^2\} \mathbf{p}_0 \cdot \mathbf{p}_0^H + E\{\|\mathbf{a}_{m+1}\|^2\} \mathbf{p}_1 \cdot \mathbf{p}_1^H + \sigma_n^2 \mathbf{I} \quad (3)$$

式中  $\mathbf{I}$  为单位矩阵。

从式 (3) 可以得知  $\mathbf{R}$  有两个较大的特征值，且对应的特征向量分别为  $\mathbf{p}_0$  和  $\mathbf{p}_1$ 。假定各信息符号间不相关，噪声为加性高斯白噪声且与信号不相

关,接收到的信号信噪比为负,  $T_s$  已经估计得到,其他参数未知。

## 2.2 仿真验证

信噪比为-8dB 的高斯白噪声环境下,扩频序列取周期为 31 的  $m$  序列,采样周期与码元周期相同,仿真结果如图 1~图 4 所示。

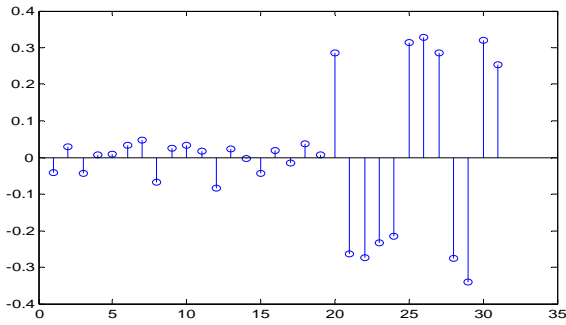


图 1 特征向量 1

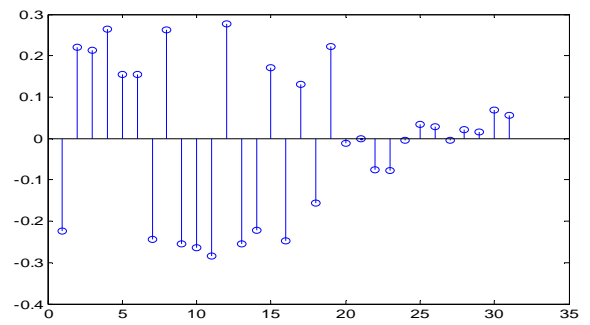


图 2 特征向量 2

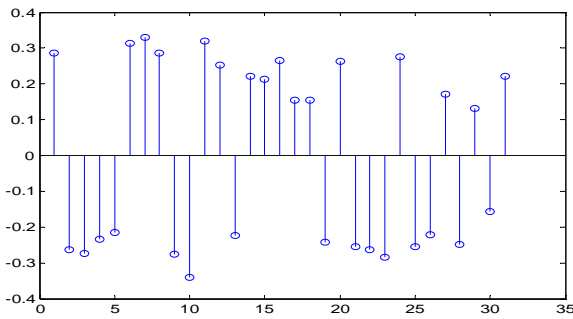


图 3 估计出的序列

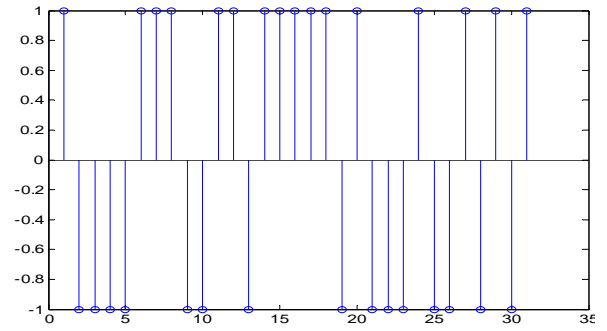


图 4 原扩频序列

## 3 扩频周期的估计

### 3.1 工作原理

基带 DS 信号可以表示为  $x(t) = c(t)d(t) + n(t)$ , 其中

$c(t) = \sum_{i=-\infty}^{\infty} c_i q(t - iT_c)$ ,  $c_i \in \{-1, 1\}$  为扩频序列;

$d(t) = \sum_{j=-\infty}^{\infty} d_j q(t - jT_0)$ ,  $d_j \in \{-1, 1\}$  为信息序列,  $q(t)$  是一个码元波形, 且有  $T_0 = NT_c$ ,  $N$  是扩频序列位数,  $T_0$  为扩频序列周期。  $n(t)$  为零均值高斯白噪声, 其方差为  $\sigma^2$ 。

根据文献[8], 信号  $x(t)$  的功率谱的二次处理结果为:

图 1 为最大特征值对应的单位特征向量, 图 2 为第二大特征值对应的单位特征向量, 图 3 是估计出的序列, 从图 3 很容易得到与图 4 中相同的序列。仿真结果与文献[5]中的结果相符, 说明基于矩阵分解的扩频序列估计方法在已知扩频序列周期时对扩频序列有很好的估计性能。

$$\begin{aligned} \hat{S}_x(e) &= |DFT\{S_x(f)\}|^2 \\ &\cong \left| T_c \sum_{k=-\infty}^{\infty} \left( 1 - \frac{|e - kNT_c|}{T_c} \right) \right|^2, |e - kNT_c| \leq T_c, k = 0, \pm 1, \pm 2, \dots \end{aligned} \quad (4)$$

由式(8)可知, DS 信号的功率谱作二次处理后, 信号能量聚集在一些尖锐的三角形脉冲序列处, 间距为扩频序列周期的整数倍。

### 3.2 仿真验证

信噪比为-12dB 的高斯白噪声环境下, 扩频序列为从  $m$  序列中截取的周期  $N$  为 200 的序列, 采样周期取码片周期的 4 倍, 每位信息码元由一个周期的扩频序列扩频, 得到的仿真结果如图 5 所示。

从图 5 中可以很容易估计出序列的周期, 该结果与文献[4]中的仿真结果相符。将数据分段求二次

功率谱后进行叠加求平均值,在更低的信噪比条件下也能估计出扩频序列的周期。说明二次功率谱检测法有很好的估计性能。

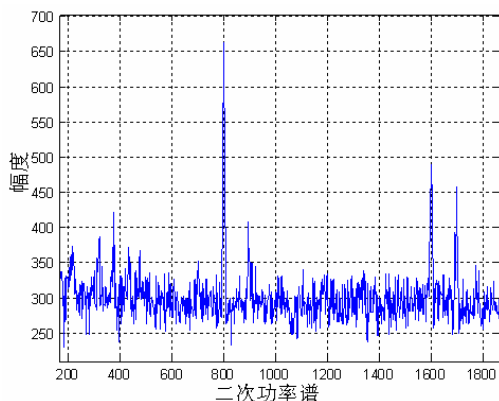


图5 二次功率谱检测曲线

$M=N\pm 2$ 、……、 $M=N\pm 30$  进行仿真,仿真发现,利用二次检测法检测的结果都为扩频序列的真正周期  $N$ ,而不是实际对信息码元扩频的码片的个数  $M$ 。由于篇幅,只给出如图 6 在  $M=230$  时的仿真结果。

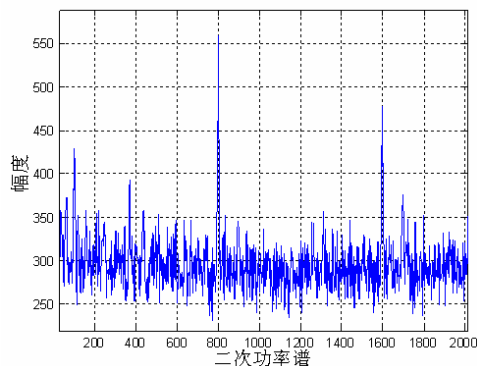


图6 二次功率谱检测曲线

由图 6 可知,仿真结果与图 5 相同。说明上面分析正确,二次检测法只能检测扩频序列的周期,不能检测实际对信息码元扩频的码片长度,只要该长度不是扩频序列的周期,利用二次检测法估计的结果就不能为进一步估计扩频序列服务。

## 4.2 对基于矩阵分解的扩频序列估计法的影响

假设扩频序列的周期为  $N$ ,实际对信息码元进行扩频的码片个数为  $M$ , $M=N+n$ , $n<N/2$ 。

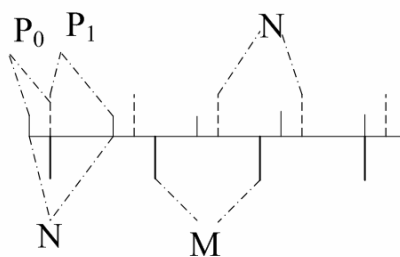


图7 扩频码片分配示意图

图 7 中短竖线间为周期为  $N$  的扩频序列,虚线竖线表示按周期  $N$  对扩频序列进行分段时的情况,此时接收到的每段数据都可以用  $\overset{u}{p}_1$  和  $\overset{u}{p}_0$  (见第 1.1 节)表示。长竖线间表示用  $M$  个码片对信息进行扩频时的情况,此时取  $N<M$ ,由图可见,在很短的几个数据段中,由于  $M$ 、 $N$ 、 $P(Ts-t_0)$ 、 $P_{t_0}$  四个数字间的关系特别复杂,接收数据与  $\overset{u}{p}_1$  和  $\overset{u}{p}_0$  之间的关系已经不能用某一通用的表达式表示。

## 4 直接序列扩频调制的改进措施

由第 1、2 节可知,在信噪比为  $-8\text{dB}$  的高斯白噪声环境下,利用功率谱的二次处理法和基于矩阵分解的扩频序列估计法,可以很好地估计出非合作方直接序列扩频信号所用的扩频序列,从而轻易截获其传送的信息。

由于以上检测方法都是基于一个最基本的假设:用扩频序列的一个周期对每个信息码进行扩频。功率谱的二次处理法实际上利用了扩频序列的周期自相关特性,自相关函数在周期的整数倍处产生的局部最大值,在二次功率谱密度函数中表现出来,从而检测出扩频序列的周期。基于矩阵分解的扩频序列估计法利用矩阵分析工具,将非同步下接收到的每段长度为扩频序列周期的信号分成两部分,分别与扩频序列中的两部分有关,从而估计出扩频序列。

设扩频序列的周期为  $N$ ,本文提出用不等于(大于或小于)  $N$  个扩频码片对一个信息码元进行扩频的方法,破坏以上两种方法的理论基础,在一定程度上提高直接序列扩频信号的隐蔽性。

### 4.1 对功率谱的二次处理法的影响

信噪比为  $-12\text{dB}$  的高斯白噪声环境下,扩频序列为从  $m$  序列中截取的周期长度  $N$  为 200 的序列,采样周期取码片周期的 4 倍。对一个信息码元进行扩频的码片的个数为  $M$ ,分别取  $M=N\pm 1$ 、

由式(2)、(3)可知,基于矩阵分解的扩频序列估计法是建立在 $\hat{p}_0$ 、 $\hat{p}_1$ 的基础上的,如果对信息码扩频的码片长度 $M$ 不等扩频序列周期 $N$ ,则自相关矩阵 $R$ 的特征值与 $\hat{p}_1$ 和 $\hat{p}_0$ 的关系变模糊,最大特征值与 $\hat{p}_1$ 和 $\hat{p}_0$ 没有必然联系,该方法已不能正确估计出扩频序列。

信噪比为-8dB的高斯白噪声环境下,扩频序列取周期为31的 $m$ 序列,采样周期与码元周期相

同,对一个信息码元进行扩频的码片的个数为 $M$ ,分别取 $M=N\pm 1$ 、 $M=N\pm 2$ 、……、 $M=N\pm 10$ 进行仿真,仿真发现,在利用基于矩阵分解的扩频序列估计法已不能正确估计原扩频序列。由于篇幅,只给出 $M=32$ 时,用基于矩阵分解的扩频序列估计法得到的最大和第二大特征值所对应的特征向量。

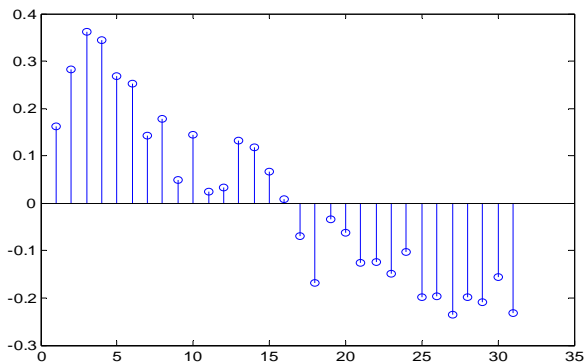


图8 特征向量1

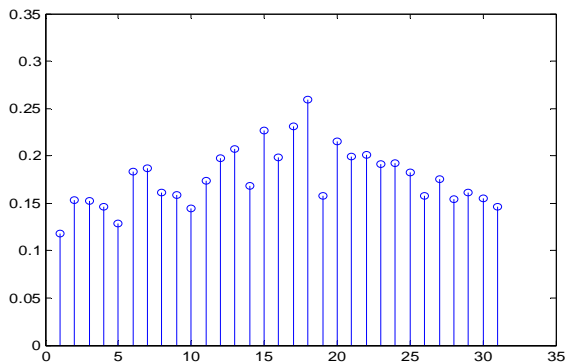


图9 特征向量2

由图8、9可知,只要稍微改变对信息码元进行扩频的码片的长度,只在原来扩频序列周期的基础上加1,用基于矩阵分解的扩频序列估计方法就不能得到正确的估计结果。通过多次仿真验证,在对信息码元进行扩频的码片的长度 $M$ 不等于扩频序列周期 $N$ 时,基于矩阵分解的扩频序列估计方法不能发挥作用。

## 5 结论

文章针对功率谱二次处理法可以估计出直接序

列扩频信号中扩频序列的周期,而基于矩阵分解的扩频序列估计方法在已知扩频序列的周期情况下可以正确地估计出扩频序列值,提出利用不等于扩频序列周期长度的码片对信息进行扩频的方法,从理论分析和仿真结果都验证了这是一个有效的方法,能解决这两种方法对直接序列扩频的隐蔽性造成的威胁,提高了直接序列扩频信号的隐蔽性。

参考文献(略)

作者联系方式

通信地址:解放军理工大学通信工程学院研究生二队

邮政编码:210007

联系电话:025-80827310

# 基于审计的数据库统计推理攻击发现

袁震

**摘 要：**在信息社会和知识经济迅速发展的今天，数据库中信息的价值越来越被认为是财富的聚宝盆，因而它的安全变得越来越重要。通过对数据库访问日志的分析，提出了发现数据库统计推理攻击的方法，可以帮助管理员改进数据库访问策略，提高数据库的安全。

**关键词：**数据库安全；网关；统计查询；推理攻击

## 1 引言

当前在安全领域，对网络和操作系统的安全研究得比较多，但对数据库及其应用程序的安全问题研究得比较少。由于数据库中的访问目标数据库、库表、记录与字段是相互关联的，字段与字段的值之间、记录与记录之间也是具有某种逻辑关系的，存在通过推理从已知的记录或字段的值间接获取其他记录或字段值的可能。而在操作系统中一般不存在这种推理泄露问题，它所管理的目标（文件）之间并没有逻辑关系。这就使数据库的访问控制机制不仅要防止直接泄露，而且还要防止推理泄露的问题，因而使数据库访问控制机制要比操作系统的复杂得多，需要为防止推理攻击而限制一些可能的推理路径<sup>[1-3]</sup>。

## 2 基本思想和原理

数据库能为用户查询提供统计信息，但为了保护个体的隐私，需要限制用户的使用，使用户只能

取得统计信息，并且没有查询序列充分到能够推理出任何个体的信息的地步。一旦个体信息暴露，则认为数据库受到了危害。控制统计推理是一件很困难的事情，因为仅靠设置权限是不够的，需要把所有已经释放的查询结果都存储起来，使得在释放一个新统计之前能够与所有存储的结果进行比较控制。这样做会严重地削弱数据库的效率和可应用性，而且几乎是不可能做到的<sup>[4]</sup>。目前控制统计推理攻击的机制分为两类：一类是限制统计的机制<sup>[5]</sup>，一类是加噪音机制<sup>[6]</sup>。

本文采用审计的方法来控制统计推理<sup>[7]</sup>，利用如图 1 所示的数据库安全网关（DBSG）<sup>[8]</sup>，过滤用户的查询请求，确保用户只能获得被安全策略允许的敏感数据。DBSG 截取目的地址为敏感数据库的 IP 数据包，分析其是不是用来查询的包，如果是则将其中的查询语句提取出来，将其存放在日志中，同时按照预先定义好的安全策略，判断查询请求是否合法。日志中记录了用户所有的操作，可以用来分析数据库是否受到攻击，改进数据库的安全策略，提高数据库的安全性。

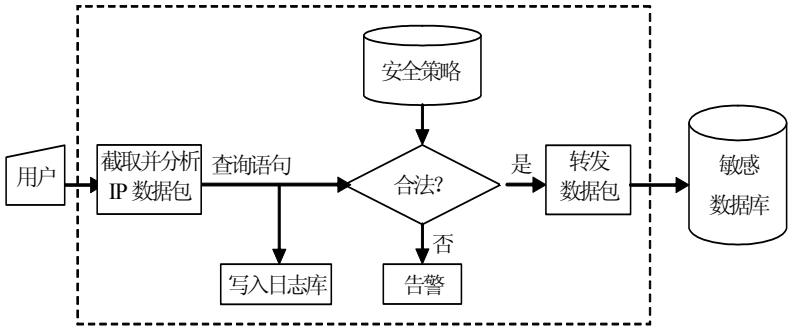


图 1 数据库安全网关示意图

审计记录的行为包括数据库管理员、安全管理员和一般用户的所有行为，包括登录、修改、删除、查询等行为。审计的内容包括主体、客体、操作类型、发生的日期和时间、主体登录地点（IP地址）。

我们把用户提交的每一条命令结合与之相关的其他属性，形成一条审计记录，存放在日志库中。每条审计记录包含的字段如表1所示，其中Type字段记录用户的登录（login）、退出（logout）和执行的数据库操作（修改、删除、查询），Command字段记录完整的SQL语句。

表1 审计记录包含的字段

用户名	时间戳	主机IP	用户IP	操作类型	命令
Username	Timestamp	HostIP	UserIP	Type	Command

现在的关系型数据库管理系统大多采用SQL语言。SQL的查询语句基本格式如下：SELECT〈属性名表/表达式表〉FROM〈基表/视图名表〉WHERE〈查询条件〉GROUP BY〈属性名表〉HAVING〈分组后查询条件〉ORDER BY〈属性名表/属性列序号表〉ASC/DESC。SQL提供的主要统计函数有：COUNT, SUM, AVG, MAX, MIN。

统计值是对有公共属性的记录子集算出的，子集由特征公式指定。特征公式对应数据库查询语句中WHERE子句的条件表达式，将任何属性名和常量或属性名和属性名用比较运算符连接起来就构成基本的条件表达式；再在条件表达式前加NOT、或两个条件表达式之间用AND或OR连接起来可以构成一些较复杂的条件表达式。根据SQL语句的这些特点，可以对日志中的查询语句进行分析。首先，将用户进行的统计即有统计函数的查询语句找出来；然后，分析统计查询的特征公式之间有没有相互关联关系，从而判断有没有遭到攻击。

### 3 数据库的统计推理攻击方法

设特征公式 $C$ 是在属性值上应用算子OR（ $\vee$ ），AND（ $\wedge$ ）和NOT（ $\neg$ ）的任意逻辑公式， $q(C)$ 是满足特征公式 $C$ 的数据记录的统计函数，如 $Count(C)$ 表示满足特征公式 $C$ 的记录个数。设 $N$ 为库中数据记录的总数， $|C|$ 为满足特征公式 $C$ 的个数。

#### 3.1 小查询集和大查询集攻击

如果一个用户 $U$ 知道某个体 $I$ 在数据库中且满足特征公式 $C$ ，又 $Count(C)=1$ ，那么 $U$ 应用式

(1) 查询

$$Count(C \wedge D) = \begin{cases} 1 & \text{蕴含} I \text{ 有特征} D \\ 0 & \text{蕴含} I \text{ 没有特征} D \end{cases} \quad (1)$$

即知 $I$ 是否含有特征 $D$ 。类似地，应用 $Sum(C, A)$ 即可求出 $I$ 的属性 $A$ 的值。

这一类型的攻击对于查询集大小不是1时也可能有效， $Count(C)>1$ 时，若 $Count(C \wedge D)=Count(C)$ ，则 $I$ 也必满足 $D$ 。为了防止此类攻击，必须限制对小查询集进行统计。下面介绍的几种攻击都是在限制了对小查询集进行统计后，进一步采取的攻击。

#### 3.2 个体追踪者攻击

假设一个用户知道一个个体 $I$ 由特征公式 $C$ 唯一地刻画，要确定 $I$ 是否也有特征 $D$ 。因为有查询集大小控制机制， $Count(C \wedge D) \leq Count(C) = 1 < n$ ，不能利用 $Count(C \wedge D)$ 和 $Count(C)$ 的异同的方法来确定 $I$ 是否有特征 $D$ 。但若 $C$ 能够分解成两部分，即 $C=C_1 \vee C_2$ ，并且 $n \leq Count(C_1 \wedge C_2) \leq Count(C_1) \leq N - n$ 。记 $T=C_1 \wedge \neg C_2$ ，可得：

$$Count(C) = Count(C_1) - Count(T) \quad (2)$$

$$Count(C \wedge D) = Count(T \vee C_1 \wedge D) - Count(T) \quad (3)$$

如果 $Count(C \wedge D)=0$ ， $I$ 没有特征 $D$ ；如果 $Count(C \wedge D)=Count(C)$ ， $I$ 有特征 $D$ 。如果 $Count(C)=1$ ， $I$ 的属性 $A$ 的值可根据 $Sum(C, A) = Sum(C_1, A) - Sum(T, A)$ 算出，偶对 $\{C_1, T\}$ 称为 $I$ 的个体追踪者。

#### 3.3 通用追踪者攻击

如果一个通用追踪者是一个满足 $2n \leq |T| \leq N-2n$ ， $n \leq \frac{N}{4}$ 的特征公式 $T$ ，则可求出 $q(C)$ ：

$$q(C) = \begin{cases} q(C \vee T) \vee q(C \vee \neg T) - N \\ 2N - q(\neg C \vee T) - q(\neg C \vee \neg T) \end{cases} \quad \begin{matrix} |C| < n \\ |C| > N - n \end{matrix} \quad (4)$$

如果不知道 $|C|$ 的大小, 可先试一试哪一个式子的查询集是允许的, 然后继续进行。

### 3.4 线性系统攻击

$$\text{设 } H \text{ 是 } m \times M \text{ 矩阵, } X = \begin{bmatrix} x_1 \\ \vdots \\ x_N \end{bmatrix}, Q = \begin{bmatrix} q_1 \\ \vdots \\ q_m \end{bmatrix},$$

这里 $q_i$ 是 $\text{Sum}(C_i)$ 形式, 凡通过建立线性方程 $HX=Q$ 达到泄露的攻击都称为线性系统攻击。为了进一步研究线性系统攻击, 引入统计数据库的键指定查询模型: 假定数据库中每一记录都有一个整数键, 键指定查询的特点是每次查询其查询集 $C$ 由 $k$ 个记录的键 $\{i_1, \dots, i_k\}$ 指定,  $k$ 是固定的。如果数据库中的每一记录 $I$ 是唯一地由特征公式 $C$ 所识别, 那么任何键表 $\{i_1, \dots, i_k\}$ 能够表达作特征公式 $C_{i1} + \dots + C_{ik}$ 。所以, 如果一个数据库能用键表指定查询泄露, 也就能用特征指定查询泄露。这说明了数据库的易损性。不过, 这是在键表能译作特征公式的前提下作出的, 如无此前提, 特征指定查询不能精确地控制查询集的构成成分。因此, 用特征达到泄露可能比用键要困难得多。

## 4 统计查询的相关性

一个统计查询系统可以用三元组来表示 $A=(R, Q, C)$ ,  $R$ 为数据库中所有记录的集合,  $Q=\{q_1, q_2, \dots, q_n\}$ 表示日志中统计查询语句的集合, 函数 $C: Q \rightarrow R^+$ ,  $C(q_i)$ 表示 $R$ 中满足 $q_i$ 查询条件的记录集合, 称为 $q_i$ 的查询集。

定义 1: 对于查询 $q_i, q_j$ ,  $i \neq j$ ,  $1 \leq i, j \leq n$ , 如果 $C(q_i) \cap C(q_j)$ 不为空, 则称 $q_i, q_j$ 相互关联, 记为 $q_i \langle q_j$ 。

定义 2: 满足以下条件的集合 $B$ 称为相互关联查询集合。这些条件有

- 1)  $B \subseteq Q$ ;
- 2)  $\forall q_i \in B, \exists q_j \in B, i \neq j, q_i \langle q_j$ ;
- 3)  $C(B) = \bigcup_{q_j \in B} C(q_j), \forall q_k \notin B,$

$C(q_k) \cap C(B)$ 为空。

## 5 发现攻击的算法与流程

发现 $A$ 中相互关联查询集合的算法如下, 其中: “ $||$ ”表示集合的模运算, 即集合中元素的个数。

输入: 统计查询系统 $A$

输出: 相关联的事务集合

初始化: 建立集合 $L = \{l_1, l_2, \dots, l_n\}$ ,

$l_k = \{q_k\} (k=1, 2, \dots, n)$ ,  $\text{flag} = \text{false}$

① if  $|L| = 1$  then 转⑩;

②  $k=1$ ;  $n=|L|$ ;  $\text{flag} = \text{false}$ ;

③ if  $C(l_k) \cap C(l_n)$ 不为空 then 转⑧;

④  $k++$ ;

⑤ if  $k < n$  then 转③;

⑥ if  $|l_n| > 1$  and  $\text{flag} = \text{false}$  then 输出 $l_n$ ;

⑦ 转⑨;

⑧  $l_k = l_k \cup l_n$ ;  $\text{flag} = \text{true}$ ;  $l_k$ 中的查询与

$l_n$ 中的查询相关联, 将它们合并;

⑨ 从 $L$ 中删除 $l_n$ ; 转①;

⑩ if  $|L| > 1$  then 输出 $l_1$ ;

⑪ end.

例: 设有查询 $q_1, q_2, q_3, q_4$ ,  $C(q_1) = \{1, 2\}$ ,  $C(q_2) = \{1, 3\}$ ,  $C(q_3) = \{2, 3\}$ ,  $C(q_4) = \{4\}$ , 上述算法的执行如下:  $L = \{\{q_1\}, \{q_2\}, \{q_3\}, \{q_4\}\}$   
 $\rightarrow L = \{\{q_1\}, \{q_2\}, \{q_3\}\} \rightarrow L = \{\{q_1, q_3\}, \{q_2\}\}$   
 $\rightarrow L = \{\{q_1, q_2, q_3\}\}$ , 输出 $\{q_1, q_2, q_3\}$ 。

假如用户进行的查询相互关联, 则可根据上节的介绍判断采取了何种攻击。具体流程如图 2 所示。

## 6 结束语

本文采用审计的方法, 将相互关联的查询挑选出来, 集中在一起提供给数据库管理员。管理员通过对相互关联的查询进行分析后, 判断是否有记录被泄露, 并增加对某些查询的限制, 同时也对那些试图获取敏感信息的用户追究责任, 降低其信任度。本文主要分析了数据库由于多次统计造成的推理泄露, 然后根据数据库的审计日志, 找出所有进行攻击的用户操作记录, 通过对这些操作的分析, 改进数据库的策略, 提高数据库的安全。

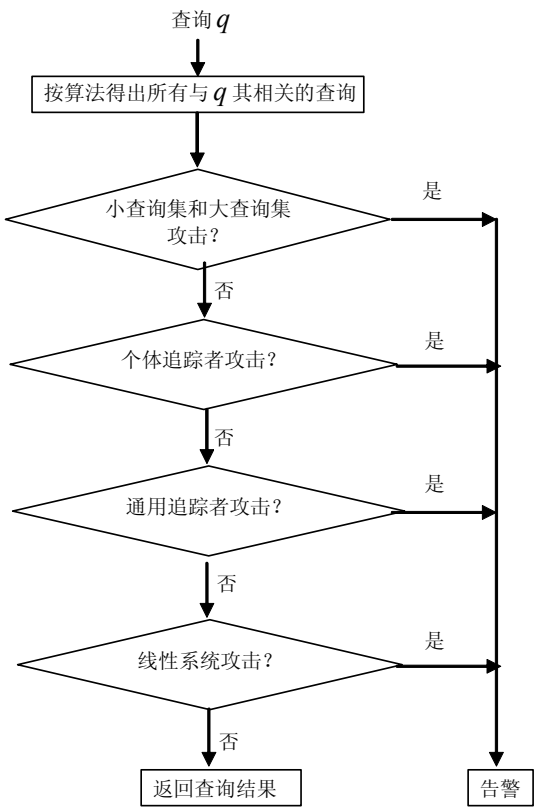


图2 攻击判断流程图

参考文献

[1] 肖军模, 刘军, 周海刚. 网络信息安全[M]. 北京: 解放军出版社, 2003:256-286.

[2] THURASINGHAM B. Data mining, national security, privacy and civil liberties[J]. ACM SIGKDD Explorations Newsletter, 2002, 4 (2) :1-5.

[3] YI R, LEVITT K. Data Level Inference Detection in Database Systems[C] // Proc of the 11th IEEE Computer Security Foundations Workshop, Rockport, MA, USA: IEEE Computer Society Press, 1998: 179-189.

[4] MALVESTUTO F M, MOSCARINI M. Computational issues connected with the protection of sensitive statistics by auditing sum-queries[C] // Proc of IEEE Scientific and Statistical Database Management (SSDBM'98) . MA, USA: IEEE Computer Society Press, 1998:134-144.

[5] MALVESTUTO F M. Statistical Database Security under a Query-Overlap Restriction[C] // Joint ECE/Eurostat work session on statistical data confidentiality.Luxembourg, Eurostat, 2003:4-5.

[6] LI Yingjiu, WANG Lingyu, Jajodia S. Preventing Interval-based Inference by Random Data Perturbation [C]// Proc. Workshop on Privacy Enhancing Technologies (PET) . San Francisco, CA:Springer April 2002:160-170.

[7] CHIN F Y, OZSOYOGLU G. Auditing and inference control in statistical databases[J]. IEEE Trans. on Software Engineering, 1982, 8 (6) : 574-582.

[8] 王雪平, 刘松鹏, 张峰, 等. BDEGATE: 一个数据库网关原型的研究与构造[J]. 计算机工程, 1999, 25 (12) : 73-75.

作者联系方式

通信地址: 南京市后标营 18 号总参第六十三研究所  
邮政编码: 210007  
联系电话: 025-80827681



# 指挥信息系统数据中心灾难恢复预案的制定和演练研究

张明安

**摘 要:** 本文介绍了指挥信息系统数据容灾体系建立过程中应急预案编制和演练的内容及管理,列出了指挥系统数据中心连续运转保障机制的建立、指挥业务连续运行保障规范与灾难恢复预案的关系、指挥信息系统灾难恢复预案的关键内容、总体典型流程等,并以例子说明指挥信息系统数据恢复步骤,文章还给出影响指挥系统数据中心容灾体系建设及灾难恢复的因素等。

**关键词:** 数据中心; 数据容灾; 灾难备份; 数据库; 灾难恢复; 灾难恢复预案; 容灾演练

## 1 引言

### 1.1 概述

随着各类指挥信息系统建设的普及与发展,关键的系统服务中断造成比以往更加严重的影响,信息系统的业务连续性管理得到各级机构的高度重视。持续、安全的数据支持对指挥信息系统数据中心十分重要,作为指挥信息系统核心和关键的数据资源,迫切需要构建数据容灾体系。

指挥信息系统数据中心容灾体系建设中明显存在“重建设、轻演练”的问题,即大部分的时间、经费用于数据中心的场地、硬件、软件等的建设,往往忽视系统建成以后应急预案的制定和演练,一旦系统需要在紧急情况下需要主备切换,常常导致切换流程不清、系统混乱、不知所措的情况发生。本文针对这一问题,主要介绍了数据容灾体系建立过程中应急预案编制和演练的内容及管理,列出了指挥系统数据中心连续运转保障机制的建立、指挥业务连续运行保障规范与灾难恢复预案的关系、指挥信息系统灾难恢复预案的关键内容、指挥信息系统灾难恢复总体典型流程等,并以例子说明指挥信息系统数据恢复步骤,文章还给出影响指挥系统数据中心容灾体系建设及灾难恢复的因素等。

### 1.2 数据容灾的重要指标和和构成

#### 1.2.1 数据容灾重要指标

指挥系统容灾的等级大体上讲<sup>[1]</sup>,容灾可以分为3个级别:数据级别、应用级别以及业务级别。数据级别容灾的关注点在于数据,即灾难发生后可

以确保用户原有的数据不会丢失或者遭到破坏。本文主要关注数据级别的容灾。

灾难恢复(disaster recovery)一般指将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态,并将其业务功能从灾难造成的不正常状态恢复到可接受状态,而设计的活动和流程。

数据中心灾难备份系统有两个重要指标:RTO和RPO。

- 恢复时间目标(RTO)<sup>[1]</sup>: recovery time objective,灾难发生后,信息系统或业务功能从停顿到必须恢复的时间要求。
- 恢复点目标(RPO)<sup>[1]</sup>: recovery point objective,灾难发生后,系统和数据必须恢复到的时间点要求。

一般来说,对于重要的指挥系统,灾备数据中心在灾难宣布后数据服务启动时间根据系统的重要程度科学制定,时间越短,灾备系统建设成本越高;采用硬件的阵列的数据复制在速度方面有明显优势(需要卷快照策略配合)。

#### 1.2.2 数据中心容灾备份系统构成

数据中心灾难备份系统建设是一项周密的系统工程,一个完整的灾难备份系统主要由数据备份系统、备用数据处理系统、备份中心基础环境和完善的灾难恢复预案(计划)组成。

##### ● 数据备份系统

在灾难备份系统建设中,数据备份是灾难备份系统最基本的要素和关键,如何将数据完整地实时复制到灾难备份中心,是灾难备份建设中需要重点考虑的事项。

##### ● 备用数据处理与通信网络系统

备用数据处理系统是指在灾难恢复时需配备的

主机、存储系统、网络系统、应用软件。

● 灾难备份中心基础环境

灾难备份中心是指配备了包括备份处理系统等各种资源以在灾难发生时接替业务系统运行的计算机处理中心。

● 灾备系统管理和恢复预案

为保证灾备系统的 7x24 小时的系统可靠性，使灾备系统能与指挥信息系统保持一致，需要制定规范的管理制度并执行，如：安全管理、运维管理、恢复管理、变更管理等。灾难恢复预案是为了规范灾难恢复流程，使得灾难发生后能够快速恢复业务处理系统运行和业务运作。

以下仅就数据中心灾难恢复管理和预案的制定提出具体的细节进行讨论。

2 指挥系统数据中心灾难恢复预案制订

2.1 指挥系统数据中心连续运转保障

指挥系统数据中心建设的同时，需配套完善指挥业务连续运行保障规范和编制指挥信息系统灾难恢复预案（包括了按照任务要求进行系统切换）。并且，在交付用户前进行演练，交付用户时，将制定的《指挥信息系统数据中心灾难恢复预案》随系

统一并交付，交付用户后，需要定期组织保障部门进行指挥信息系统灾难恢复预案的演练，确保灾难到来时，指挥信息系统的正常运转。

数据中心连续运转保障见 0。包括日常运行、维护和系统正常切换和灾难恢复。

(1) 日常运行维护

数据中心日常运行中的管理包括：监控管理、安全管理、客户管理、质量管理几个部分。除了以上的管理外，还需要进行经常性的系统测试、系统验证、系统演练、灾难恢复预案的修订。

(2) 系统正常切换和灾难恢复

一旦发生灾难或按任务要求系统切换，灾难恢复预案启动，灾难恢复基本步骤包括：应急响应、灾难恢复、重续运行、重建恢复。

三个重要名词：

【BCP】：“指挥信息系统指挥业务连续运行保障规范”。

【BCM】：指挥信息系统指挥业务连续运行管理。

【DRP】：《指挥信息系统数据中心灾难恢复预案》。数据中心灾难恢复预案定义<sup>[3]</sup>是指指挥信息系统灾难恢复过程（或按照任务要求进行系统切换过程）中所需的任务、采取的行动、数据和资源文件，用于指导相关人员在预定的灾难恢复目标内恢复指挥信息系统支持的关键指挥业务功能。

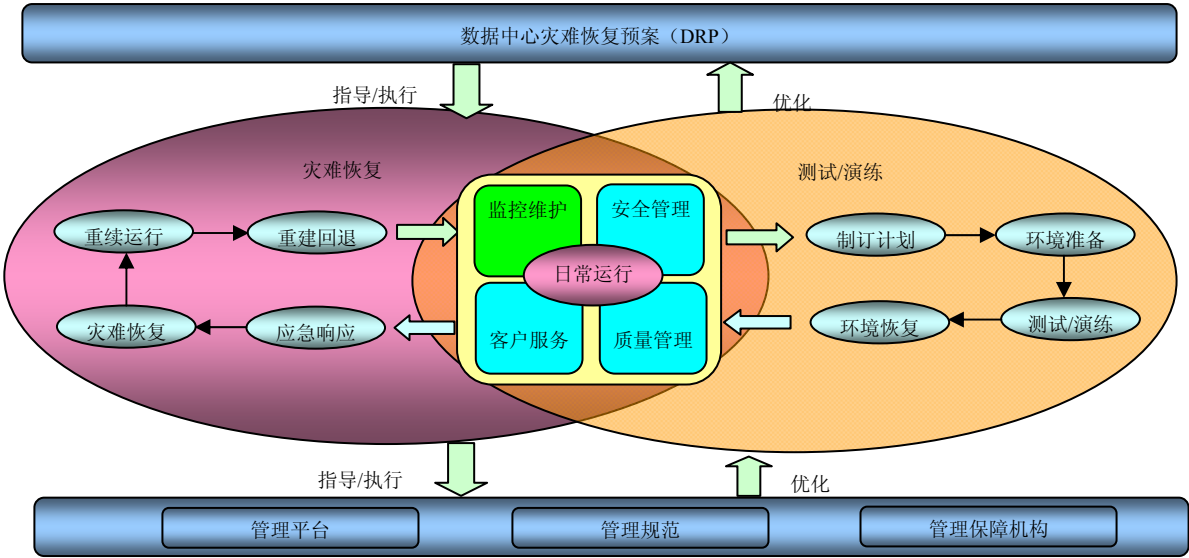


图 1 数据中心连续运转保障

2.2 指挥业务连续运行保障规范与灾难恢复预案的关系

图 2 和表 1 描述了《指挥信息系统指挥业务连续运行保障规范》(BCP) 与《指挥信息系统数据中心灾难恢复预案》(DRP) 的关系。其中, 指挥业务连续运行保障规范包括: 指挥信息系统指挥业

务连续运行保障规范、各分系统已制定的(或修订过的)场地设施应急预案、各分系统已制定的(或修订过的)业务系统应急预案、指挥信息系统指挥业务恢复工作流程。BCP 与 DRP 的目的和关注点不同, DRP 是 BCP 的 IT 部分内容。BCP 可以作为 BCP 的附件单独成册, 也可作为 BCP 的一个章节。

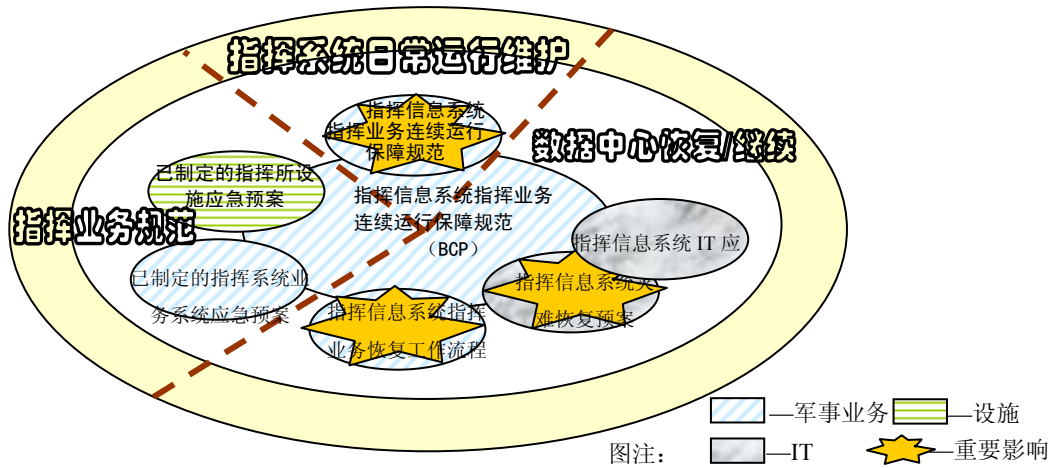


图 2 指挥业务连续运行保障规范与灾难恢复预案的关系

表 1 指挥业务连续性计划与灾难恢复预案的关系

计划分类	目的	关注点	相互关系
《指挥信息系统指挥业务连续运行保障规范》(BCP)	提供重大中断恢复期间维持重要的指挥业务运行的规程	指挥信息系统指挥业务连续运作, 关注点是指挥信息系统指挥业务	BCP 与 DRP 的目的和关注点不同, DRP 是 BCP 的 IT 部分内容。一般来说, DRP 可以作为 BCP 的附件单独成册, 也可作为 BCP 的一个章节
《指挥信息系统数据中心灾难恢复预案》(DRP)	提供在紧急事件后在备用站点恢复目标系统数据的详细规程	关注点是指挥信息系统(数据完整性)	

一般来说, 编制《指挥信息系统数据中心灾难恢复预案》(DRP) 至少要求包含以下几方面。

- 整体要求: 指整体上对制定预案统一要求;
- 制订过程要求: 具体到每一个操作细节;
- 日常宣贯、培训和演练要求: 列出培训计划和时间表;
- 管理要求: 对数据中心灾难恢复预案的组织机构设立以及计划、演练进行全面的描述。

编制《指挥信息系统数据中心灾难恢复预案》(DRP) 的意义体现在以下几方面:

- 规范灾难应对的处理流程, 减轻或降低灾难时的混乱状况;
- 指导恢复操作, 缩短恢复时间;
- 最小化决策量, 降低决策风险;

- 灾难恢复能力测试及演练的标准和依据;
- 增强抵御灾难的能力, 提高指挥信息系统的安全感。

2.3 指挥信息系统数据中心灾难恢复预案的关键内容

图 3 是指挥信息系统数据中心灾难恢复预案的关键内容示意图。一般来说, 指挥信息系统数据中心灾难恢复预案的主要内容:

- 灾难恢复的目标和范围
- 灾难恢复的组织架构
- 灾难预警处理流程
- 灾难决策流程
- 灾难通报流程

- 灾难恢复处理流程
- 计划内备份系统切换处理流程
- 灾后回退处理流程
- 人员联系清单等相关信息资料

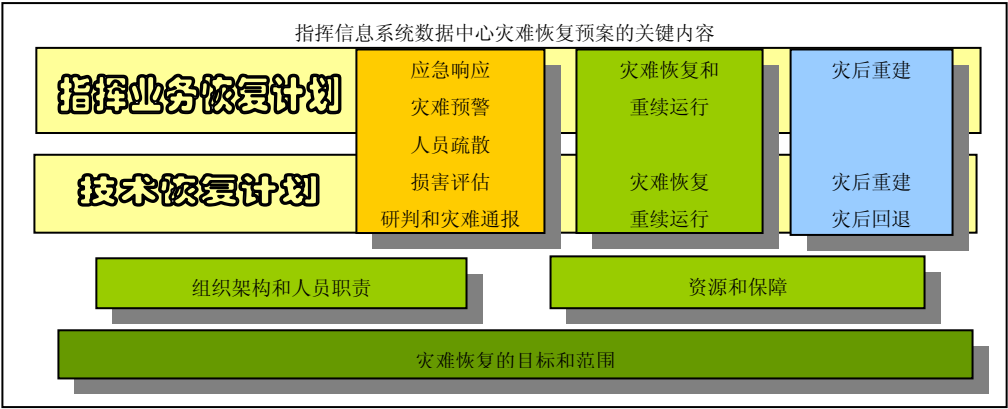
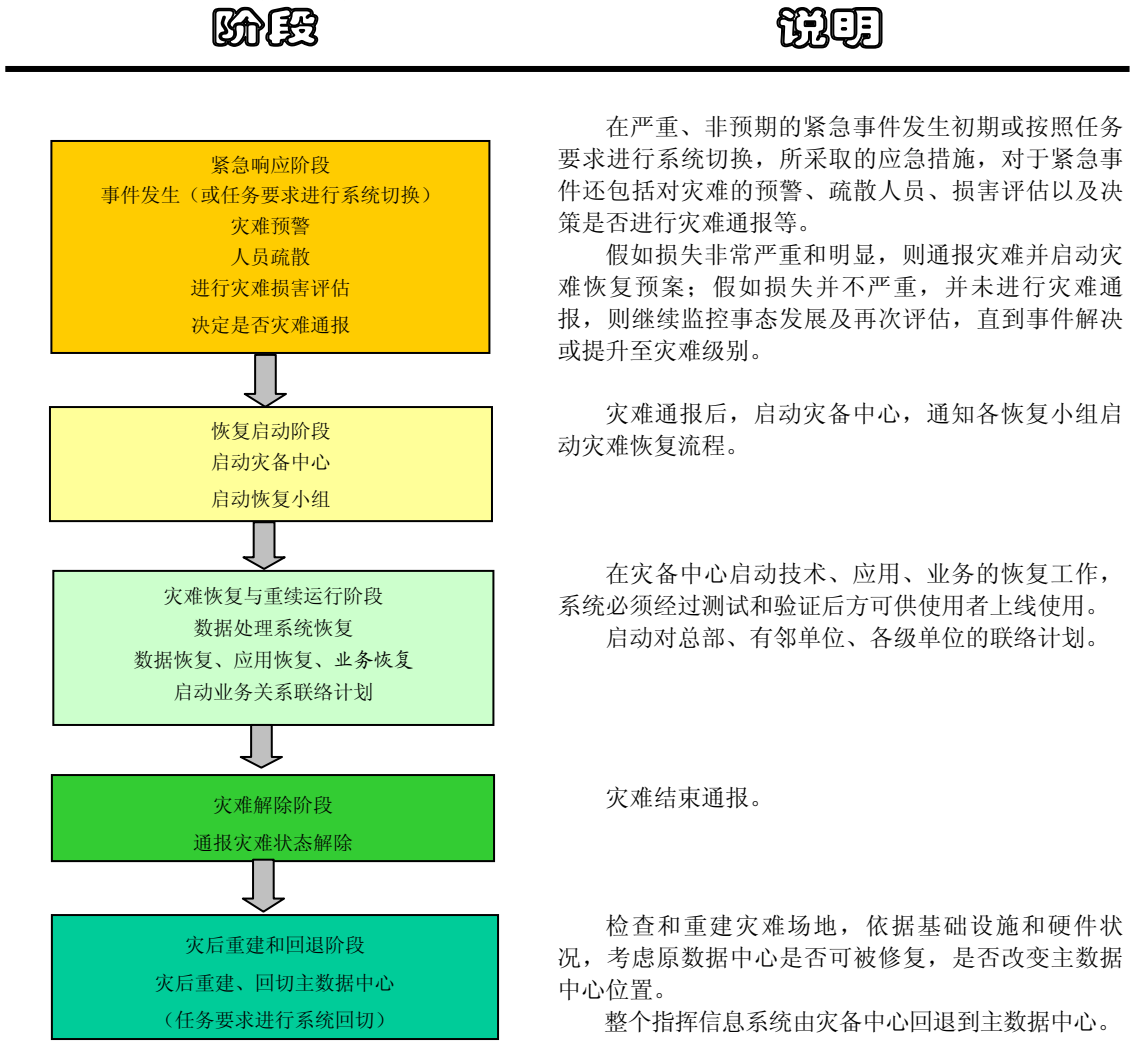


图3 指挥信息系统数据中心灾难恢复预案的关键内容

2.4 指挥信息系统灾难恢复总体典型流程

指挥信息系统灾难恢复总体典型流程在数据中心建设阶段由管理单位、使用单位、保障单位共同

制定，指挥信息系统灾难恢复总体典型流程说明如下。



2.5 指挥信息系统数据恢复演练步骤

灾备系统建成后，当灾难发生或按照任务要求进行系统切换时，数据的恢复是关键，只有完成恢复，才表明灾备的建设是真正有作用的，信息系统的风险降到了最低。灾备系统建设完成一并提交的《指挥信息系统数据中心灾难恢复预案》中对灾难发生时数据恢复组织、操作、步骤、用时等进行详细的阐述，《指挥信息系统数据中心灾难恢复预

案》必须进行用户培训、反复演练，形成固定的演练流程后方可在实际的任务中进行系统间切换或当灾难到来时从容实施数据中心灾难恢复。

以下以图 4 的数据中心与备份数据中心间的连接关系示意图为例，介绍数据中心与备份数据中心间切换及灾难恢复。其中①为主数据中心；②为同城灾备数据中心；③为远程异地灾备数据中心。

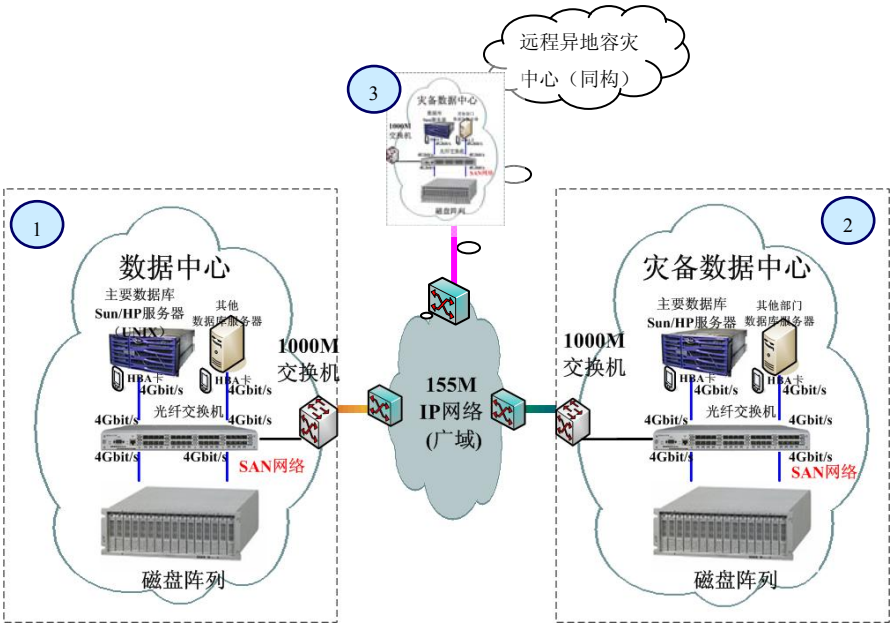


图 4 数据中心与备份数据中心间的连接关系示意图

主数据中心，如果需要切换至同城灾备数据中心，步骤如下（图中①→②为例）。

- 1) 指挥信息系统主数据中心①的应用停止运行（人为操作或灾难性故障）；
- 2) 中断指挥信息系统主数据中心①与同城灾备中心②的数据复制[break]；
- 3) 中断指挥信息系统主数据中心①与远程异地灾备数据中心③的数据复制[break]；
- 4) 应用系统在同城灾备数据中心②启动、运行；
- 5) 将指挥信息系统主数据中心①、远程异地灾备数据中心③设为同城灾备中心②的灾备中心。（在以任务方式切换条件下，主数据中心①有效，当主数据中心①发生灾难失效时，仅远程异地灾备数据中心③设为同城灾备中心②的灾备中心。）
- 6) 同城灾备中心的数据②可增量复制回主数据中心①（主数据中心①由于任务发生切换时，本

步骤有效）[resync]；

- 7) 同城灾备中心的数据②可增量复制回远程异地灾备数据中心③[resync]。

灾难结束后应用系统切换回主中心的操作步骤如下（图中②→①为例）。

- 1) 人为停止同城灾备中心②应用系统的运行；
- 2) 指挥信息系统主数据中心①应用系统启动、运行；
- 3) 将同城灾备中心②、远程异地灾备数据中心、③设为主数据中心①的灾备中心。
- 4) 指挥信息系统主数据中心①与同城灾备中心②、远程异地灾备数据中心③恢复正常数据复制。



## 2.6 指挥信息系统数据中心灾难恢复预案的定期回顾检查及优化服务

(1) 数据中心灾难恢复预案的定期回顾检查的目的

指挥信息系统数据中心灾难恢复预案的定期回顾检查及优化服务目的是对用户的各项灾备管理制度和流程,如日常工作流程、切换流程、回切流程,定期回顾运作状况、存在问题和新的需求和战略远景,并提出优化建议,保证系统指挥业务的连续性。对于灾备组织架构,定期回顾运作状况、存在问题和新的需求战略远景,并提供优化建议。

(2) 数据中心灾难恢复预案优化服务的方法步骤

- 制定《灾难恢复体系定期回顾与优化计划》(本文略)
- 召开灾难恢复体系定期回顾会议确定《灾难恢复体系定期回顾与优化计划》
- 按照修订的计划进行实施,在实施结束后将提交《灾难恢复体系定期回顾与优化报告》。

## 3 影响指挥系统数据中心容灾体系建设及灾难恢复的因素

影响指挥系统数据中心容灾体系建设及灾难恢复的因素体现在以下几方面。

1) 按照常规信息系统集成项目的建设思路实施灾备项目,认为 IT 集成部分完善即可而不考虑

组织管理、“指挥信息系统数据中心灾难恢复预案”的制定、演练。

2) 对 RTO 和 RPO 的期望过高,建议根据业务的关键程度及数据的完整性要求来定义。

3) 一些指挥信息系统,IT 部门基本承载了日常业务运营,可以说 IT 就是业务。这些 IT 部门的灾备项目,目前往往集中在 IT 软硬件的恢复,是不完整的灾难恢复计划,加上没有其他灾难恢复预案计划的配合,导致很多人疑惑在灾难发生时 IT 部门的灾难恢复机制能不能发挥作用。

4) 认为应对罕见灾难投入的预算较高,投入产出和谐。

5) IT 部门的灾难恢复预案计划没有和相关业务部门的灾难恢复计划很好地衔接。

6) 目前采用的成本效益分析方法不成熟。

## 4 结束语

目前国内各类信息系统(包括指挥信息系统)已经或准备开始建设容灾备份体系,建设容灾备份体系的关键是数据容灾,系统集成后,最重要的是指挥信息系统数据中心灾难恢复预案,以及对指挥信息系统数据中心灾难恢复预案的用户培训、反复演练、不断修改完善指挥信息系统数据中心灾难恢复预案,只有将指挥信息系统数据中心灾难恢复预案进行不断的演练并固化演练程序,才能当下达灾备转移时从容应对系统切换时带来的各类问题,保证系统平稳切换,为指挥信息系统提供持续、安全的数据支持。

参考文献(略)

作者联系方式

通信地址:北京市海淀区万寿路3号

邮政编码:100036

联系电话:010-66974179 13051655544

# 一种基于管理员权力限制的数据库安全增强技术

张锐 刘军

**摘 要:** 针对目前数据库管理员权力过大的情况, 提出数据库管理员监控机制。该监控机制在不影响数据库正常工作的前提下, 增加了对管理员权力的限制。分析表明, 该机制能够较大幅度地限制因管理员出现问题而对数据库造成的破坏, 进一步保证数据库的安全性。

**关键词:** 数据库安全威胁; 数据库安全策略; 监控机制

## 1 背景知识

伴随计算机性能的快速提升和数据库技术的进一步发展, 越来越多的人开始关注数据库的安全问题。人们更多关心的是对数据库合法用户的非授权访问和非法用户对数据库安全造成的威胁, 往往忽视了数据库管理员 (Database Administrator, DBA) 对数据库造成威胁的可能。DBA 的职责是维护数据库系统的正常运行, 不必具有很高的信息访问权。而目前 DBA 却常常拥有所有的访问权。当 DBA 账号和密码被非法人员获得后, 将对数据库造成巨大威胁。所以, 需要对 DBA 的权力进行一定的约束。

有关 DBA 带来的安全隐患, 一般情况只涉及了 DBA 账户和口令的保护, 关心 DBA 账户不被非法盗用。但是, 如果 DBA 存在对数据库安全的故意威胁, 则可能造成无法估量的损失。一旦怀有恶意的人想利用 DBA 账户对数据库进行破坏, 则轻而易举。对于这种危险, 它几乎没有任何保护。

目前, 针对该问题大多数人给出的是将 DBA 权力一分为三的方法<sup>[1,2]</sup>, 以此来削弱 DBA 的权力。本文从对 DBA 实行监控的角度, 提出一种有别于上述文献中给出的三权分立的解决办法。

## 2 数据库安全介绍

### 2.1 数据库的安全威胁

威胁数据库的主要因素有以下几点: ① 物理环境带来的安全威胁。② 敏感信息的泄露和信息被篡改。③ 安全机制不够完善, 存在可被利用的安全漏洞和弱点。④ DBA 专业知识的欠缺, 安全

保护机制不能被很好的利用, 从而造成安全威胁。

⑤ 可能受到来自网络黑客和网络病毒的威胁<sup>[3]</sup>。

### 2.2 数据库的安全要求

对数据库的安全要求, 究其根本其实就是对数据库存储信息的安全要求。主要有三个方面: 要求数据库存储的信息不被不相关人员看到的数据的保密性; 要求数据库存储的信息保持一种完整的或是未受损的状态的数据的完整性; 要求合法授权的用户在他需要的时候能够正确使用这些信息的数据的可用性。为了保护数据库信息的这三条性质, 要求数据库具有用户认证、访问控制和可审计性等安全机制<sup>[3,4]</sup>。

## 3 基于管理员权限监控的数据库安全增强方案

### 3.1 安全增强方案的设计思想

为了避免 DBA 账户被恶意使用, 在数据库系统中增加一个监督机制, 用来监督 DBA 的行为 (如图 1 所示)。监控机制是数据库管理系统 (Database Management System, DBMS) 的一个组成模块。从安全角度考虑, 将之从 DBMS 中提取出来单独放置, 使 DBA 无法触及。

当 DBA 对数据库进行某种操作, 并且这些操作威胁到数据库安全的时候, DBMS 将把该项操作完整地记录下来, 且不对数据库进行实质的修改。同时, 向监督机制报警。监督机制检查该项操作。经审核无误后, 向 DBMS 发出允许修改的批准书。DBMS 在得到来自监督机制的批准书后, 验证其真实性。为真, 则提取先前记录下的 DBA 修改

数据库的操作记录，对数据库进行真实的永久性的修改。如果，DBMS 没有收到来自监督机制的批准书，记录下来的 DBA 操作将被搁置一旁不予理

睬，直到收到该操作的批准书。如果收到的是来自监控机制的拒绝信息，DBMS 就删除该条记录。

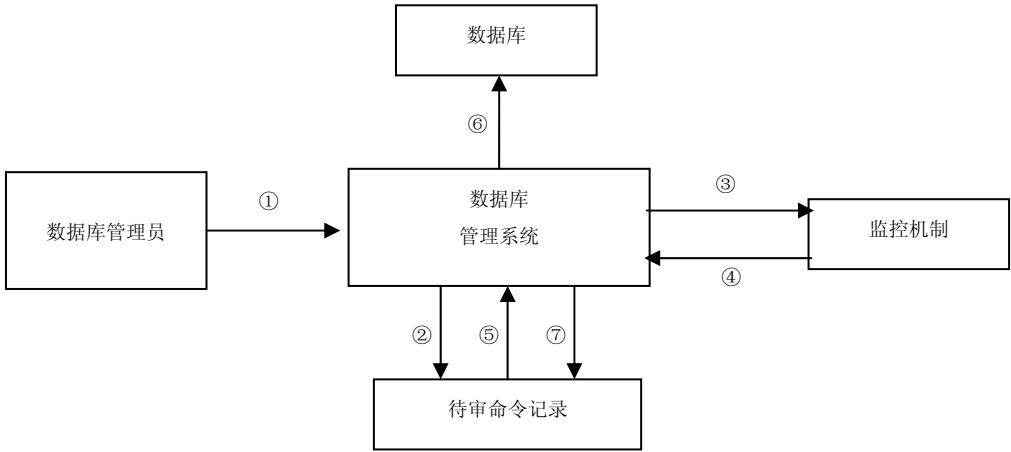


图 1 监控流程图

- 步骤：
- ① DBA 企图对数据库进行操作；
  - ② DBMS 将这些操作记录在案；
  - ③ DBMS 向监控机制报警；
  - ④ 监控机制审核操作申请，若允许，返回批准书，执行⑤；若不允许，则返回拒绝信息，执行⑦；
  - ⑤ DBMS 接收到监控机制的批准书，从待审命令记录中提取先前记录的操作命令；
  - ⑥ 将提取出来的命令对数据库执行，删除记录，任务结束；
  - ⑦ DBMS 接收到监控机制的拒绝信息后，将

该记录删除。

3.2 安全增强方案的具体设计

3.2.1 监控模块的设计

对 DBA 的监控机制可以通过一个监控模块来实现其功能。监控模块由几个小的功能模块组成。每个小功能模块完成一个独立的任务。监控模块的结构组成如图 2 所示。虚框范围内为监控模块，左边为 DBMS，右边为安全机构。

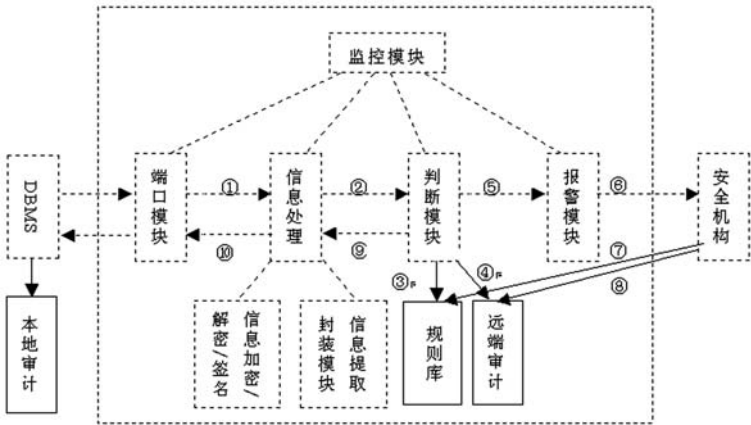


图 2 监控模块结构组成图

- 模块功能分析：
- ① 端口模块：用来接收和发送信息的模块，负责与 DBMS 之间的通信。

- ② 信息处理模块：该模块分成两个子模块。一是信息加密/解密/签名模块，负责将收到的信息解密成明文并进行身份验证，将要发送的信息加密



并对其签名；二是信息提取/封装模块，负责从收到的数据包中提取信息或者是把要发送的信息封装成数据包。DBMS 处也需有一该模块与之相匹配。

③ 判断模块：负责判断 DBA 欲执行的命令是否会对数据库构成安全威胁。

④ 报警模块：负责向安全机构报警。

⑤ 规则库：存放行为判断规则，给判断模块提供判断标准。

⑥ 远端审计：记录 DBA 的操作，含批准与未批准的。

监控模块的具体工作流程：

① 端口模块将 DBMS 发送来的信息上交给信息处理模块。

② 信息处理模块把这些信息解密并进行身份验证。身份验证通过后将里面的信息提取出来，上交给判断模块。

③ 判断模块得到信息后，根据规则库定义的规则进行判断，查看 DBA 输入的命令是否合法。不合法，则拒绝其操作，并通知报警模块需要报警给安全机构；合法，则批准其操作。

④ 判断模块将 DBA 的操作和判断结果记录到远端审计中。

⑤ 判断模块拒绝该操作时向上级报警。

⑥ 报警模块向安全机构报警。

⑦ 规则库中判断规则仅由安全机构制定。

⑧ 仅安全机构可查看远端审计内容。

⑨ 判断模块将判断结果返回给信息处理模块。

⑩ 信息处理模块将审核模块传过来的值和其他的内容封装成数据包，然后进行加密、签名处理，交给端口模块。

最后由端口模块把信息返回给 DBMS。

### 3.2.2 安全增强设计方案

首先定义规则库中的知识。将数据库命令按序编号 1、2、3...，每条命令中参数用  $x$ 、 $y$ 、 $z$ ...表示。在规则库中，限定每条命令中每个参数的值域，即为判断标准。监控模块收到信息，根据命令检查所有参数是否在其值域内。是，则符合规则；否，则不符合。

DBA 要对数据库进行操作，就需输入操作命令。此时，DBMS 将 DBA 输入的命令存放到一个指定的存储器中，同时为之设定一个 ID 号来唯一标识这条记录。但是，不使这些操作真正实施到数

据库上。

DBMS 向监控机制发出报警。该报警在监控机制看来，也可以理解为是对数据库操作的申请。信息在发送前，通信双方首先进行双向零知识身份证明<sup>[5]</sup>。双方预制一个相同的数  $x$ ，经某一单向算法  $f$  得到  $f(x)$ ，将其转换为二进制形式。DBMS 将其结果第一位  $x_1$  发给监控模块，后者将之与自己结果的第一位  $x_1'$  比较，相同则返回第二位  $x_2'$  给 DBMS，DBMS 将之与自己结果的第二位  $x_2$  比较，相同则返回  $x_3$ ，以此类推。中间若有某位不相等，则马上终止会话。会话正常结束，说明双方认证成功。相比幂指运算和模运算的零知识证明<sup>[6,7,8]</sup>，上述方法更易于实现，效率更高。而后将信息加密和签名，以防他人冒充身份发送伪造的申请和保证数据在传输过程中的安全性。因已经进行双向认证，加密算法使用 DES 即可。DBMS 将加密后的信息发送给监控机制。发送出去的信息包含本身的身份识别码、该记录的 ID 号、时间、操作命令和相关的参数等内容。

监控机制收到报警信息后，首先进行解密处理。经核实确是 DBMS 发送过来的信息后，读取内容。根据规则库规则对各命令进行判断，检查其合法性。比如，要求 DBA 不具有创建另一个 DBA 账户的权力。当监控机制读到这样的命令后，将予以拒绝。判断结束，监控机制需要把审核结果返还给 DBMS。返还回去的信息包含其本身的身份识别码、信息返还时间、原记录 ID 号、原报警时间、批准/拒绝位等内容。批准/拒绝位是用来标识该申请是否得到批准。若批准该申请，该位取值为 1，否则设为 0。返还的信息同样需要经加密处理过后才能发送出去。若拒绝其执行某项操作，则向安全机构报警。

DBMS 收到来自监控机制的返回消息，首先进行解密处理，验证其是否是监控机制发送过来的信息。经验证无误后，读取里面的内容。如果是批准书，即监控机制同意管理员想要对数据库进行的操作，允许其执行，DBMS 按照记录的 ID 号从存储器中提取该条记录，按照记录内容对数据库实行真正的操作。若是一条拒绝信息，DBMS 将根据 ID 号把这条记录从待审命令记录中删除。需要指出的是，不论 DBA 想要对数据库进行的操作有没有得到监控机制的允许，这些信息同样需要记录到 DBMS 的审计日志中去。

对于审计日志,为保护其安全,使用异地双备份审计日志机制。一个存放于本地,一个存放于异地。即便 DBA 把本地日志修改了,但是他无法修改异地的审计日志。安全机构将定期根据异地审计日志对本地审计日志进行检查。远端审计日志仅允许安全机构查看,使其安全性得到保证。如果本地审计日志与异地审计日志不相符,则认为本地审计日志已经被非法篡改,按照异地审计日志对其进行修复,从而保证了审计日志的安全。

在 DBMS 一端,也需要增加一个对监控模块进行身份认证的模块,以防止他人伪装监控模块发送给 DBMS 恶意的响应破坏数据库。

该监督机制,只具有对 DBA 行为的监督、批准和拒绝权力。只有当 DBA 企图修改数据库的时候才被调用。它不具备发起修改数据库行为的权力。

通过该监控机制,数据库的任何用户,包括 DBA,均不拥有私自执行对数据库具有安全威胁的操作的权力。因为普通用户对数据库的操作受 DBA 的监控,而 DBA 对于数据库的操作受到管理系统监控机制的监控。这样,就避免了在数据库里的一言堂情况的发生。数据库的安全得到了进一步的保证。

## 4 性能分析

若 DBA 账户被攻破或 DBA 自身操作出现问题,由于 DBA 监控机制的存在,限制了其可行使的权力。因得不到监控机制的批准,DBA 无法对数据库造成过大的或根本无法造成破坏。同时,监控机制能及时地给出响应,批准或拒绝 DBA 的某项操作,不会影响到数据库的正常工作效率。因

此,可以说该系统在保证工作效率的前提下针对 DBA 是安全的。

很多文献提出的三权分立方法,将管理员、安全员和审计员的角色分开,使之互相监督,在一定程度上是限制了 DBA 账户的权力。但是依然存在不小的隐患。只要 DBA 的账户名和密码正确,安全员就会允许其以 DBA 身份登录数据库,而 DBA 账户的安全级别最高,无论系统采用 DAC、MAC 或 RBAC 的访问控制方法<sup>[4]</sup>,都不会影响 DBA。审计员即便记录了所有的 DBA 操作,审计日志只是用于事后检查和追查责任<sup>[2]</sup>。在事后检查之前,可能 DBA 账户对数据库的实际破坏已经造成。并且,细粒度的审计很耗费时间和空间,难于实现。可见,“三权分立”只能在一定程度上禁止管理员对数据库的破坏行为。

有的文献通过“将系统的功能分布在多个相互连接的独立的处理器或模块上”<sup>[9]</sup>,利用各模块之间的相互调用来实现对数据库的操作。然而,DBA 因其安全级别之高,可以任意调用系统模块。若 DBA 账户出现问题,即便是这种分布式的结构也无法保证数据库的安全。

## 5 结束语

随着数据库存储的信息的价值的不断的提升和信息量的不断增大,数据库的安全问题越来越受到人们的重视。本文的主要思想,是把 DBA 以前非常大的权力限制到一个能够保证他正常工作又使他无法对数据库的安全构成威胁的范围内。这是通过对数据库增加的 DBA 监控机制来完成的。这样,数据库的安全范围得到了扩展,使其安全性得到增强。

参考文献(略)

作者联系方式

通信地址:解放军理工大学通信工程学院研究生1队

邮政编码:210007

联系电话:025-80828449

# 基于层次的安全事件关联模型

张潇毅 吴庆 张慧

**摘 要：**针对当前分布在网络中的各种安全设备产生的海量报警信息可能导致管理员很难从中获取有效信息的问题，文章给出了一种基于层次分析的安全事件关联模型，并将该关联分析方法与其他方法进行了对比研究。

**关键词：**事件关联；代理；知识库

## 1 引言

随着网络信息技术的发展，黑客攻击、病毒、后门和漏洞等网络安全威胁也越来越受到人们的关注。为了保证网络系统的相对安全，防火墙、入侵检测系统（IDS）、防病毒系统、漏洞扫描系统、安全审计系统等安全设备在网络系统中得到了广泛应用。虽然这些安全设备在一定程度上提升了网络的安全性能，能够在特定方面发挥一定的作用，但这些设备在使用过程中都会产生许多报警信息。这些报警信息语义级别低，在真实的报警信息中包含着大量的重复报警和误报警，再加上信息的海量，使得管理员难以在有限时间内完全分析处理所有设备上的所有报警信息，更难以识别报警的真实性，发现隐藏在这些信息背后的攻击意图。如果因为信息的海量而导致许多真实的报警信息得不到应有的关注，报警也就失去了意义。

为解决上述问题，安全事件关联已成为发展的必然趋势。文章给出了一种基于层次分析的网络安全事件关联模型，该模型保持防火墙、IDS 等安全设备的部署不变，采用一个中心节点集中统一接收这些节点上的所有报警信息，并将系统划分为四个层次：事件采集层、预处理层、关联分析层和管理报告层，然后综合运用多种关联方法从不同角度对报警信息进行统一关联分析，过滤冗余报警，辨别出真实报警，挖掘出隐藏在海量报警信息背后的攻击企图，并预测下一步攻击，同时给出关联分析的结果报告以及可能的响应措施。

## 2 事件关联的相关概念

大部分的安全事件都不是孤立产生的，彼此之间存在着某种联系，从攻击的角度出发，这种关联性是指它们是否是由同一个攻击所产生的，这种攻击行为包括单个简单攻击行为和由一系列攻击步骤组成的复杂攻击行为。这里的安全事件（此文中也称报警信息）是指由安全设备发出的一段消息，用来表示出现了违反计算机或网络安全策略的行为。事件关联分析就是从大量安全事件中寻找这种内在联系，并根据这种联系对事件进行处理。通过关联分析，可以对相同或相近的安全事件进行处理，以避免重复报警；可以挖掘深层次复杂的攻击行为，以识别有计划的攻击行为；可以提高分析的实时性，以及时做出响应。

## 3 基于层次分析的安全事件管理模型

### 3.1 部署结构

该模型通过在不同的安全设备上驻留代理，代理负责采集安全设备的报警信息，并将其转换成统一的数据格式，通过安全信道将采集到的原始报警信息发送到安全事件关联中心，安全事件关联中心根据知识库信息对报警信息进行相关性分析处理，用户通过控制终端查看关联分析结果，并对报警做出相应的决策处理。其部署结构如图 1 所示。

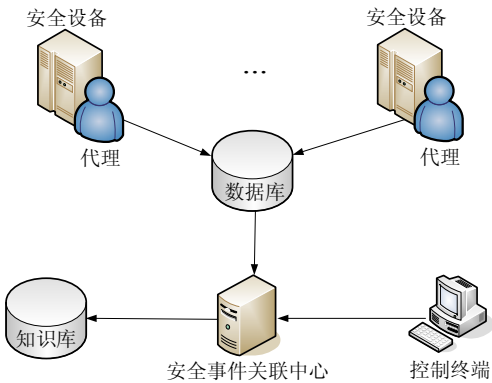


图 1 部署结构

该部署结构具有以下特点。

分布式事件采集：本模型保留设备的部署不变，通过在设备上驻留代理来实现安全事件的分布式采集，减轻了安全事件关联中心的处理负担。

集成化综合处理：能够对采集的各种类型的数据进行集中综合分析，能准确把握全局网络安全状

况，使得关联分析更加准确。

可扩展性强：能够管理各种网络安全设备，包括硬件设备和软件系统。不同的安全设备的管理可以通过驻留不同的代理来实现。如果要管理新增的安全设备，只需增加对应的代理即可，具有良好的扩展性。

跨平台：能够管理运行在各种不同操作系统上的安全设备。

3.2 功能结构

本模型对事件进行层次式分析，其结构如图所示，安全事件关联分为四个分析层次：数据采集层、数据预处理层、关联分析层和管理报告层。每一层实现不同的关联目的。

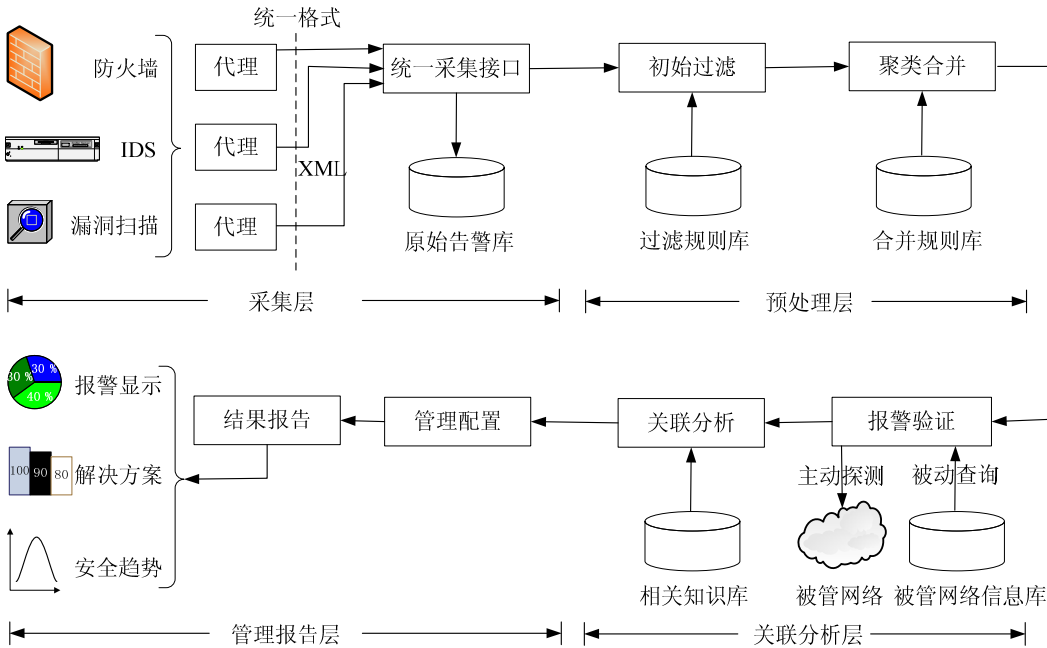


图 2 层次式事件管理模型

3.2.1 数据采集层

采集安全事件是建立关联的第一步。系统通过在安全设备上驻留代理来实现事件采集。采集代理获取各个安全设备的原始数据后，进行规范化；然后将处理后的事件传输到安全关联中心的统一采集接口模块上，进行集中存储。数据采集层在功能实现时做到接口统一、格式统一、存储统一。

3.2.2 数据预处理层

采集并规范化安全事件后，需要对其进行预处理，即去除不必要的事件和冗余事件，从而在有效信息不丢失的前提下尽可能地减少安全事件数量，提高事件处理效率。数据预处理层包含两个模块：初始过滤模块和聚类合并模块。初始过滤模块主要完成重复报警事件的过滤。比如 ping of death, syn

flood 等攻击一般会在短时间内持续重复出现很多相似的报警信息。聚类合并模块主要是按照合并规则对报警事件进行聚类合并。比如可以使用源地址、源端口、目的地址和目的端口等安全事件的属性作为指标,设定不同的条件进行聚类统计,通过聚类合并,可以有效的减少大规模扫描所产生的报警事件数量。

3.2.3 关联分析层

关联分析层是模型的核心层,包含两个模块:报警验证模块和关联分析模块。经过数据预处理层对报警数据进行过滤、聚类合并后,报警信息数量大大减少,本层主要结合被管网络的信息来对报警信息的真实性进行验证,以减少误报,另外,根据安全事件之间的相关性,对大量孤立的安全事件进行关联分析,得到更为准确的报警信息,以发现潜在的攻击意图。

(1) 报警验证模块

该模块主要通过与被管网络的信息库交互(主动或被动的方式)来进行一些较为复杂的验证处理,以识别误报警,标识那些没有获得成功的攻击所产生的报警,以减轻关联分析模块的处理负担。比如有一类误报警的产生根源是网络包内确实包含攻击特征,但对具体的目标与环境并不起作用或没有获得成功<sup>[6]</sup>。

(2) 关联分析模块

通常情况下,一次完整的攻击会按照特定的步骤(踩点、扫描、登录、提升权限等)进行,而当前大部分报警事件仅仅对应的是攻击者攻击过程中的一个步骤而已,孤立地看待单个步骤产生的报警信息是不易全面了解攻击的,这些报警信息之间存在一定的逻辑因果关系。关联分析模块就是利用安全事件之间的这种联系,来实现对安全事件的关联,再现攻击的场景,发现攻击企图。目前许多学者从不同的角度对安全事件关联分析进行了深入的研究,提出了许多不同的关联算法,比如基于统计分析的,基于关联规则的,因果关联算法等。

3.2.4 管理报告层

管理报告层作为系统的顶层直接与安全管理员进行交互,它提供友好的人机界面使安全管理员能够直观地查看事件关联结果,了解攻击过程,方便对安全事件做出处理,并调整安全策略。它包括两个模块:结果报告模块和管理配置模块。

结果报告模块负责提供丰富的事件显示和查询功能,方便管理员对非法事件和行为进行追踪和分析处理。管理配置模块负责提供知识库和安全设备的灵活管理,以及系统参数配置和策略的调整。

通过上面的阐述可以得出,系统的每一层都比下层提供了更加抽象的事件信息。数据采集层提供了局部的原始事件信息和经过规范化的事件信息;预处理层提供了过滤和合并后精简的事件信息,它可以抽象为单个设备和多个设备两个层面上的事件预处理,单个设备事件信息的预处理可以在代理上独立进行,而综合对多个设备事件信息进行预处理,可以使不同来源的事件相互补充,相互印证,有利于更好地理解事件,提供更全面的信息;关联分析层在上述基础上,进行更深入的关联操作,目标是完成攻击步骤的关联,重构攻击过程(也称攻击场景)。与单独的原始事件相比,攻击场景可以使管理员对攻击的理解更透彻;管理报告层则站在全局的角度,提供对攻击的预测和当前网络安全态势的分析。图表示了事件关联分析的抽象推理层次。

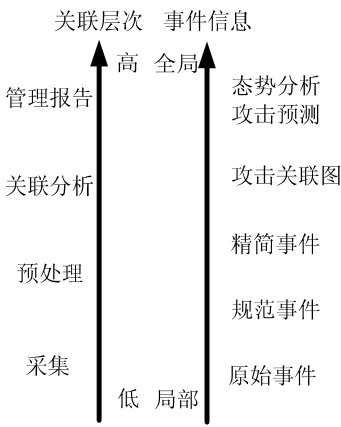


图3 关联分析的抽象推理层次

3.3 关联分析方法

目前许多学者提出的安全事件关联方法有其各自的优缺点和适用场合。因此,在关联方法实际应用中,不能只着眼于关联方法本身的优劣,还要根据具体的关联目的选择合适的方法。本文采用的关联方法遵循如下三个策略。

实时和离线相结合:支持对安全事件的实时关联,可以有效的减少事件数量,降低误报率,以便管理员及时对事件进行处理;也支持对安全事件的离线关联,重构攻击者入侵的攻击过程,为管理员

制定适当的安全策略提供依据。

横向关联和纵向关联相结合：支持对安全事件的横向关联，即根据来自不同安全设备的事件进行空间上的横向关联，或者根据攻击源、攻击目标、安全事件类型等进行事件属性间的横向关联。同时也支持对安全事件的纵向关联，即根据安全事件发生的因果关系，进行时间上的纵向关联。

综合使用各种安全事件关联方法：不同的关联方法对不同情况下事件的处理效果是不一样的，方法之间的互补性很强。要取得较好的关联效果，系统要根据目的的不同综合采用各种方法，文献中均验证了这个观点。

综上所述，本文首先通过对事件进行过滤合并和攻击验证等实时处理，减少事件数量；然后改进了文献[7]作者 PengNing 提出的因果关联方法，一是通过限定关联的时间边界提高了关联的效率，二是通过攻击验证标识了攻击未成功的攻击场景，三是利用了安全事件关联的优势即事件来源广泛，对规范化后的多源事件进行集中分析处理，提高了分析的准确性，并在一定程度上提高了检测率。采用改进后的关联方法对安全事件进行离线关联分析，重构攻击场景；最后采用统计查询分析方法对事件进行辅助分析，掌握网络安全态势。

4 实验与分析

本文使用 JBuilder 2006 和 SQL Sever 2000 作为开发工具，在 PengNing 给出的算法的基础上，对模型各层的核心功能进行了实现。为了验证模型

的有效性和可行性，本文采用 Darpa2000 数据集来对系统进行测试。实验中采用 Snort 工具直接对数据集的 Tcpdump 抓包文件进行分析，然后将产生的事件存放到 Mysql 数据库中。另外，使用 PengNing 网站上提供的 RealSecure 入侵检测系统分析 Darpa 数据得到的报警事件文件，将其导入 SQL Sever 数据库中，作为实验测试另一种安全设备的数据来源。测试所用的知识库是从 PengNing 网站上下载的。系统对这两种数据源的数据进行综合关联分析处理，并将结果和 PengNing 实现的入侵报警关联工具 TIAA (Toolkit for Intrusion Alert Analysis) 分析的结果进行比较 (TIAA 仅对单个入侵检测系统的事件进行关联)。

图 4 给出了四种技术的检测率随攻击数量的变化情况。从图中可以看出 TIAA 的检测率略低于 RealSecure，这是合理的。因为 TIAA 是在 RealSecure 报警事件的基础上进行分析的，基本上低于 RealSecure 的检测率，但也有可能高于它，比如通过更好的关联方法来发现或推理漏检的攻击。另外，本文系统的检测率要高于 TIAA，主要是因为系统对 Snort 和 RealSecure 两种设备的数据进行了综合，比仅对单一安全设备事件进行分析获得了更多的信息，但是其检测出的攻击也基本上不会高于多个设备检测到攻击的总和。同时也表明 Snort 和 RealSecure 可以相互补充，得出一个较全面的攻击情况，从而减小漏报。可以得出，通过多源事件关联，可以综合多个安全设备的事件，达到信息的相互补充，提高检测率，从而体现出事件来源的广泛是事件关联的优势。

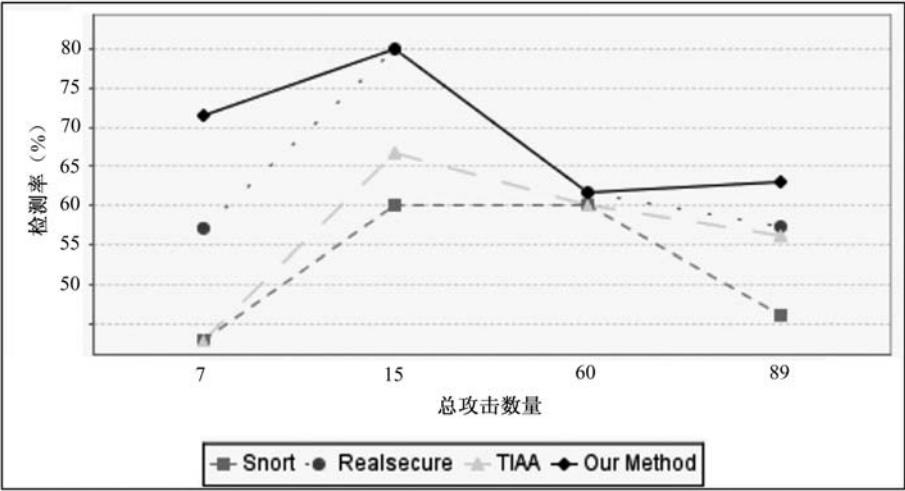


图 4 检测率比较

图 5 给出了四种技术的误报率随攻击数量的变化情况。从图中可以看出，TIAA 和本文实现的系统都大大减小了安全事件的误报率，两者在误报率上相差不是很大。Snort 和 RealSecure 在没有进行

关联分析的情况下，误报率很高，这也是现今 IDS 面临的一个普遍问题，可以考虑通过关联分析技术来解决此问题<sup>[9]</sup>。

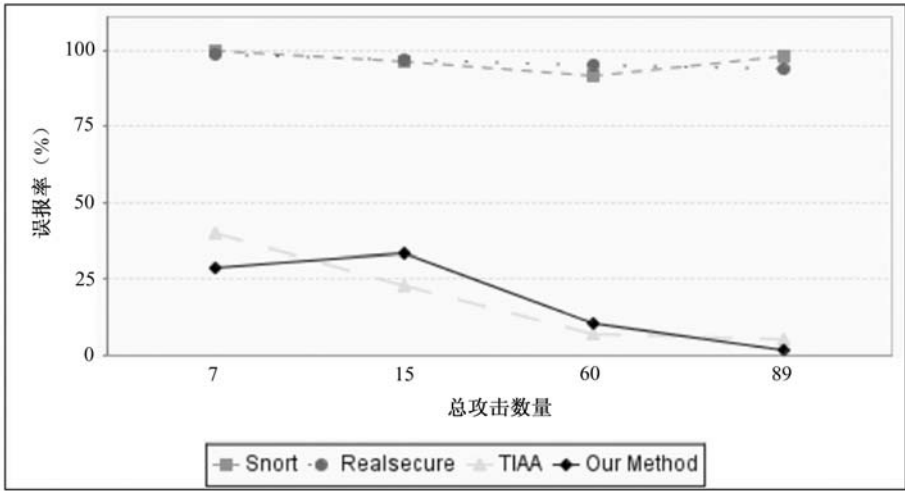


图 5 误报率比较

实验表明，系统在保证有效信息不丢失的前提下，大大减少了事件的数量，并且可以在保证或提高检测率的前提下，减小误报率，同时重构出攻击场景，方便了安全管理员进行攻击的预测、漏检攻击的发现，并为网络安全策略的调整奠定了基础。

理系统，具有不同形式的报警信息，因此能够向被管网络提供一个具有统一集成化的用户管理界面，对网络中所有的安全事件进行统一、集中监控，并能根据预定的安全策略进行及时响应的安全事件关联系统的需求将日益突出，安全事件关联也必将成为未来网络安全的综合解决方案。

5 结束语

随着不同网络安全技术和安全产品在实际网络系统中的大量应用，不同的安全设备具有不同的管

参考文献（略）

作者联系方式

通信地址：南京市后标营 18 号总参第六十三研究所  
邮政编码：210007  
联系电话：025-80827785

# 战场无线传感器网络通信多级安全策略研究

钟俊华 黄曙光

**摘 要:** 对战场无线传感器网络的通信架构的特点进行了介绍, 分析了无线传感器网络安全需求和面临的安全威胁, 在原有安全体系结构基础上提出了多级安全策略。

**关键词:** 传感器网络; 安全威胁; 安全架构; 多级安全策略

## 1 引言

随着嵌入式计算机系统和无线通信技术的发展, 无线传感器网络广泛应用于民间和军事上, 比如: 环境监控, 机器人玩具, 战场监控, 家庭和办公室位置感应无线网络, 生物医学感应器, 户外暴风雨, 海洋和天气状况的监测。在军事应用中, 传感器网络的安全保密至关重要。在数字化战场上, 战场传感器网络是由成百上千的传感器节点组成, 感知战场环境的变化。战场传感器网络可以应用于地方危险战区的监测, 战场上的目标跟踪, 灾难规避信息网络等等。

战场无线传感器网络面临各种威胁: 在信息传输过程中面临敌方对信息的监听篡改, 拒绝服务 (DOS) 攻击, 部署于敌方战场的传感器节点还将面临地方的物理摧毁等。本文将探讨无线传感器网络的安全问题并根据其特点分析一种多级安全策略。

## 2 无线传感器网络简介

无线传感器网络一般是自组大规模无线网络, 由众多的独立传感器节点组成。传感器节点间通过低能耗的无线信道相互通信。传感器节点由一个计算能力和存储空间有限的微控制器, 环境状态感知器和一个无线收发器组成, 能源储备也是十分有限。网络中没有控制管理中心, 各节点都动态地响应重要节点的错误事件。节点还能够感知位置, 并且有多跳路由的能力。实际的路由算法因为一般的路由策略都是事先定义好的而被简化处理。根据不同的用途, 不同的无线传感器网络有着不同的特性。

## 3 通信体系架构特点

在传感器网络中, 通信是通过无线方式进行的, 广播是通信的最基本方式。一个典型的无线传感器网络包含一个或多个作为外部网络接口存在的基站, 传感器节点组成路由森林, 而基站处于森林根的位置。局域广播支撑着可感知事件的数据交换, 对于构建和维持这个无线网络架构起着至关重要的作用。

无线传感器网络中的节点通过无线网络进行通信, 所拥有的计算、存储和能源储备都很有限。节点间相互的通信将消耗大量的能量, 因此节点中的系统及其应用程序的相互通信需要被降至能接受的程度。

通信协议的设计特点:

- 1) 分布式执行;
- 2) 非循环的路由方式;
- 3) 最小化路由通信;
- 4) 最小化能耗;
- 5) 网络的自主配置;
- 6) 最小化传输时延。

基本的无线通信是不安全的, 通过广播方式进行, 攻击者可以对网络进行监听, 注入新的消息, 重新发送过时消息。所发送的消息必须经过验证。传统的验证方式是通过不对称数字签名方式实现的, 但由于携带验证信息的数据包的长度太长, 并不适合无线传感器网络。许多网络采用验证信息流协议 TESLA 协议。

由于存储空间十分有限, 节点不能时刻保持所有的应用程序代码。另外, 在部署传感器节点之前, 并不知道所要运行的具体应用。在部署传感器节点后进行手工配置是不大现实的, 因此代码的可



移动性是十分必要的。

4 无线传感器网络的安全需求分析

- 1) 数据的完整性。确保接受者接受到的数据在传输过程中未被敌方篡改。
- 2) 数据的机密性。网络中收发的消息包含敏感信息（如代码，位置信息等），必须确保数据经过只有接受者才拥有的密钥加密后再发送。在网络中必须建立节点间、节点和基站间、基站和基站间的安全保密的传输信道。
- 3) 数据的可验证性。敌方可以轻易地向网络中注入消息，接受者必须能够识别信息来源安全可靠。
- 4) 数据的可访问性。传感器所收集的信息经过数据融合后可以被基站乃至用户访问到，在传输过程中而不会被阻隔。
- 5) 数据的保鲜性。敌方监听到消息后，肯能将过时的消息重新注入网络中，所以必须确保所有的消息都是最新的。主要有两种方式：第一种是消息不携带时延信息但提供部分消息排序功能的弱保鲜方式。第二种是提供一种通过请求响应方式的完全顺序消息传输的强保鲜方式。

5 所面临的安全威胁

将会来自以下几个方面的攻击威胁着整个网络的通信安全。

- 1) 敌方肯能把恶意代码注入至移动代码中，从而传播到网络中的所有节点。此时敌方将利用恶意代码摧毁整个通信网络，或者取得网络的控制

- 权。敌方也肯能将错误的感知数据传输到用户的节点中，从而形成伪装欺诈。
- 2) 节点间传输的含有位置信息的信息可以被敌方侦听拦截从而轻易定位并摧毁网络节点。对于一些静态的节点来说，其位置的信息必须在其整个生命周期都受到保护。
- 3) Denial-of-Message 攻击。传感器节点被剥夺了向其他节点发送消息的能力。敌方可以通过为每个消息回复验证的 ACK 而达到目的。
- 4) 除了节点位置信息外，敌方还可以监听应用程序之间传输的数据，包括消息的标识，时间戳，和其他信息域。但由于这种数据生命周期较短，因此其安全重要性略低于前面提到的两种消息。
- 5) Dos 攻击。恶意的节点可能对通信协议算法的攻击从而使其周围的节点做多余的运算，从而阻止数据的传输并消耗能源。
- 6) 陷害攻击。恶意的节点可以通过网络或者基站把一个好的节点标记为不可信节点从而使得可用节点变得不可用。
- 7) 阻塞式攻击。由于消息收发对于节点来说是种高能耗的操作，恶意的节点通过不断地注入错误或者无用的垃圾消息，将消耗整个网络的能源，甚至使其枯竭。

6 安全通信策略模型

无线传感器网络由于节点拥有的资源受限，为了达到资源与安全强度的折中，在安全体系结构种引入多级安全策略。

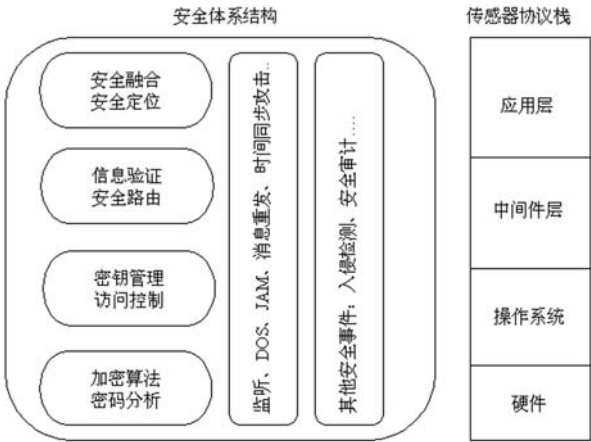


图1 安全体系结构

主要有三种数据在网络中传输：

- 1) 可移动式代码；
- 2) 无线网络传感器的位置信息；
- 3) 应用程序之间的数据传输。

根据定义的三种数据将会在网络中传输，定义一种多级安全通信策略模型。这种模型是基于群组密钥的密钥加密系统。

由于节点数据传输过程中我们加入的安全策略，涉及到一些简单或者复杂的运算，不仅会增加数据的传输时延，而且会消耗系统更多的能源。针对所传输数据对安全性的要求要求并不相同，为了将消耗的能源最小化，将采取不同的安全级别。

三种安全级别：

1) 针对包含有移动代码等敏感数据消息的传输所采用的安全策略。

2) 针对包含有位置信息的信息的传输所采用的安全策略。

3) 针对应用程序传输的一般消息传输所采用的安全策略。

以上三种级别的安全策略将采用各种不同的算法，或者使用相同的算法不同的参数使运算的负荷自适应变化。后者可以节省代码的存储空间。

传感器网络通信架构中的多播通信模型使得群组密钥成为一种更好的选择。因为，假如每个通信的节点对都维持一个或一组密钥，通信的模式将改变，节点间传输的数据量将会极大地增加。在不改变网络通信模型的前提下，我们选择采用群组密钥加密的通信方式。

所有的节点刚开始将共享相同的初始主密钥群组。群组的规模主要取决于整个网络的生命周期的长短。采取动态创建和传播密钥的方案是所采取的协议必须保证每个节点均能接受到一个密钥，对于这种网络是不适用的。

在网络的生命周期中，同一时刻总有一个密钥处于激活的状态。所有的节点运行同一种伪随机数发生器算法产生的数字来索引到密钥表中去，并且处于周期性的同步运行状态。针对三种不同的安全级别，相应地采用的是三种不同的密钥方案，这些密钥都是从主密钥中衍生出来的。

## 6.1 安全级别一

在传感器网络部署至战场后，包含有可执行的移动代码的消息将被发送到各个节点。这种分发操

作的频率较低，因此他允许系统采取更强的加密手段进行加密。为了保护这种信息的安全传输，各个节点将采用当前活动主密钥。需要访问网络的节点必须拥有一整套的主密钥，相应的为随机数发生器程序和使用该程序时的种子参数。一旦拥有后，该节点便可以向网络中注入移动代码。因此敌方突破此安全防护级别便有向网络中注入恶意代码的机会。

## 6.2 安全级别二

在传感器网络中，位置信息将包含在大部分的消息中。对于此类包含了位置信息的信息的保护将影响整个网络的安全。节点将采用基于位置的密钥组来加密此类消息。但一旦被突破，敌方便可以定位网络中所有的节点。根据传感器网络节点部署的环境不同，可以采取不同的方式来区分对待处于危险敌方地域和处于相对安全地域的节点。

传感器网络所覆盖的区域将被划分为不同的单元区域。处于相同的单元区域的节点共享同一基于位置的密钥。在单元区域之间将留出边界区域，其大小应该和数据传输距离相等。处于边界区域中的节点必须含有所有邻接单元区域的密钥，这样才能确保所有需要通信的节点均含有相同的密钥。单元区域必须足够大，这是由网络通信所采用的协议算法的局部性特征决定的，从而保证了单元区域间的通信量保持较低的水平相对于总的通信量来说。把整个区域采用相同的尺寸划分为各个单元区域将有助于节点更迅速方便地发现其处于同一个单元区域的其他成员节点。可将整个传感区域划分为六棱形的单元区域，在此引入扩展单元区域的概念。所谓扩展单元区域即为将原始单元区域各条边向外延伸节点数据传输距离后构成的单元区域。节点可能处于原始单元区域中，也肯能处于扩展单元区域中。节点通过将自己的位置与各个扩展单元区域进行比较从而决定自己处于哪几个扩展单元区域中。为了与所处的扩展单元区域中的节点通信，处于扩展单元区域的节点必须拥有其所属的所有扩展单元区域的密钥。

## 6.3 安全级别三

对于应用程序之间传输的消息数据，采用较弱的加密方式，相应所需的能耗也比较低。再者由于此类消息的交互较为频繁，也限制了系统采用强的

高能耗的加密算法,但相应的安全性不如以上所述的两个级别。所采用的密钥是从当前主密钥通过哈希函数产生的。由于当前主密钥的周期性变更,此级别的密钥也相应周期性地在变更。

求,所面临的安全威胁。战场传感器网络,一方面拥有的各种资源都十分有限,另外面临各种软硬的杀伤威胁,因此既要达到资源的高效利用,又必须考虑到安全问题,多级安全策略模型可适应此类网络的特点,达到效率与安全的折中优化。

## 7 结论

在本文中我们讨论了战场传感器网络安全需

### 参考文献

- [1] David D. Hwang, Bo-Cheng Charles Lai, Ingrid Verbauwhede, *Energy-Memory-Security Tradeoffs in Distributed Sensor Networks* In Proc. 3rd International Conference on Ad-Hoc Networks and Wireless.
- [2] Jonathan M. McCune Elaine Shi Adrian Perrig Michael K. Reiter *Detection of Denial-of-Message Attacks on Sensor Network Broadcasts* In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May, 2005.
- [3] Jing Deng, Richard Han, and Shivakant Mishra *Enhancing Base Station Security in Wireless Sensor Networks* In the 2nd IEEE International Workshop on Information Processing in Sensor Networks (IPSN 2003).
- [4] Christer Englund and Henrik Wallin *RFID in sensor network* CHALMERS UNIVERSITY OF TECHNOLOGY. Goteborg, Sweden, April 2004.
- [5] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava *On Communication Security in Wireless Ad-Hoc Sensor Networks* In: Proc. of the 11th IEEE Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2002).
- [6] Budhaditya Deb, Sudeept Bhatnagar and Badri Nath *Information Assurance in Sensor Networks* WSNA 2003
- [7] ADRIAN PERRIG, ROBERT SZEWCZYK, J.D. TYGAR, VICTOR WEN and DAVID E. CULLER *SPINS: Security protocols for sensor networks* In: Proc. of the 7th Annual Int'l Conf. on Mobile Computing and Networks. Rome: ACM Press, 2001. 189-199.

### 作者联系方式

通信地址: 安徽合肥电子工程学院研三队

邮政编码: 230037

联系电话: 13865961581

## 第 4 部分

# 信息系统应用开发

# 关注办公文档格式规范UOF

戴浩

**摘要:** 经 ISO 审核的 ODF 和 OOXML 均是支持 XML 语言的办公文档格式。本文简要回顾了这两类标准产生的背景, 指出其竞争的实质是对信息资源的控制。今年颁布的国家标准 UOF 与 ODF 兼容, 并具有较好的开放性和继承性, 需要采取切实措施, 积极支持和采用符合国标的国产办公软件。

**关键词:** 办公文档; 开放式标准; XML

## 1 标准之争

开放文档格式 ODF (Open Document Format) 是在 SUN 公司的 Star Office 基础上发展起来的, 是开放源代码项目 Open Office 2.0 的文档格式, 其宗旨是改变办公软件相互封闭、文档格式互不兼容的情况, 它同时支持文字处理、电子表格、演示文稿、制表制图和图形编辑等办公应用软件。在 SUN 和 IBM 等公司的推荐下, 非赢利的标准化机构“结构化信息标准促进组”OASIS (Organization for the Advancement of Structured Information Standards) 成立了技术工作组, 决定将基于 XML 的 ODF 作为未来的办公文档的标准格式, 并提交给国际标准化组织 ISO, 2006 年 5 月已被 ISO 审核通过, 成为文档格式的国际标准 ISO/IEC 26300。OASIS 是在 SUN、IBM、Oracle 等 36 个成员创建的开放文档格式联盟 (ODF Alliance) 发展起来的, 目前已拥有 600 多个组织、5000 多名成员。我国的红旗中文 2000 等企业也参加了 OASIS。美国马萨诸塞州政府、德国慕尼黑市政府、新加坡国防部、法国财政部等政府机构曾公开宣布支持 ODF 标准。

为了摆脱长期以来文档标准受制于人的被动局面, 从 2002 年起, 在国家电子政务总体组的指导下, 由红旗中文 2000、永中、金山、中标普华等国内知名的字处理软件厂商和研究机构组成了中文办公软件基础标准工作组, 他们制定的《中文办公软件文档格式规范》UOF (Unified Office document Format, 简称“标文通”) 已于 2007 年 4 月获得国家标准化委员会正式批准, 作为国家推荐标准 GB/T 20916-2007, 并从 9 月起全面实施。UOF 也是基于 XML、具有纯文本特点的文档格式标准。

自 20 世纪 90 年代以来, 微软 Office 软件使用的.doc、.xls 和.ppt 格式已成为事实上的文档标准, 并一直保持其在办公软件领域的垄断地位。迫于办公软件从封闭转向开放的趋势和压力, 微软开始意识到要从传统的二进制格式转向 XML 文档格式, 但在这方面动作较慢, 微软仅用了一年左右的时间, 匆匆地将自己的一套基于 Office 2007 文件格式规范——OOXML (Open Office XML) 提交给了欧洲计算机制造商协会 (ECMA), 于 2006 年 12 月成为欧洲行业协会的标准, 并得到了佳能、爱立信、富士通、HP 等厂商的支持。微软以此为跳板, 又向 ISO 提出申请, 利用标准审批的“快速通道”, 想尽快成为第二个文档格式的国际标准。

2007 年 9 月初, ISO 公布了该标准评估流程初始阶段的投票结果。在 69 张有效票中, OOXML 共得到 51 张支持票, 占 74%, 离获得通过的要求仅差一票。中国和印度、巴西等国投了反对票。英国、法国投了有条件的反对票。他们表示, 在最终评估流程中, 如果微软能对 ISO 提出的技术评论中需要 OOXML 改进的问题能得以解决, 它们也将支持 OOXML 成为国际标准。在由 37 个成员组成的 ISO/JTC1 委员会中, 微软的支持率为 53%, 也没有达到法定的 2/3 多数。估计在 2008 年 3 月的最终投票中, OOXML 很有可能被通过, 因为目前 90% 以上的电子文档都使用微软的格式, 我们必须承认这一事实。

尽管这三类标准均基于 XML 语言, 但在功能和格式规定中仍有差异, 为真正实现文档格式的全面兼容, 标准之间的转换将不可避免。我国在制定 UOF 标准时, 就考虑到与 ODF 的互通和融合, 两者之间的相似度较高。去年, IBM 资助北京大学开展 ODF 和 UOF 之间格式转换的研究。而微软的

OOXML 的标准文本有 6000 多页，基本上是 Office 2007 技术指标的翻版。微软的合作伙伴已开发出 OOXML 和 ODF 之间的转换器 (Translator) 或插件；为示友好，微软还支持北京航空航天大学进行 UOF 和 OOXML 之间的转换研究。但由于 OOXML 与前两个标准差异较大，这些转换都是非对称的。目前，三类标准实际上形成了两大阵营。我国 IT 界许多有识之士曾呼吁要支持和推广应用国家标准 UOF，反对 OOXML 成为国际标准，其主要原因是标准之争的背后，隐藏着与开发者利益攸关的市场竞争，对文档使用者来说，牵涉信息资产的控制权和安全问题。

## 2 利害攸关

标准是规范软件发展的重要指南，也是软件业的制高点，谁掌握了标准，谁就有主动权。文档格式的标准之争，实质上就是由谁来制订软件领域的游戏规则，是共同制订还是由一家制订？由于文档是信息的重要载体，这场文档格式的标准之争也是信息资源控制权之争，影响是极为深远的。长期以来，微软的私有文档格式已成为事实上的标准，并且挟垄断操作系统之优势，免费提供 Office，占领了绝大多数的市场份额，用户被锁定于微软的 Office。封闭的文档格式一直是困扰国产办公软件产业的发展，自主创新的重大技术壁垒就是微软 Office。我军早期研制的 BG 办公软件，国内知名企业金山公司的 WPS 软件，都很难与微软的办公软件抗衡。为了生存，国内办公软件企业被迫把很多精力放在与微软文档格式的兼容性上。但微软的文档格式不公开，使得这些企业始终处于暗中猜测和模仿状态，每当微软版本升级时，国内企业还要不断地跟踪和适应微软变化后的文档格式，加之专利的制约和知识产权的陷阱，致使国内办公软件企业长期停滞不前、无法发展壮大。

当你用微软的 Word 2003 打开 10 年前精心保存的办公文档时，你会发现文档中有乱码或根本打不开。什么原因呢？因为当年创建文档时的办公软件与现有版本不能“精确兼容”。无形中你已丧失了历史数据的拥有权和控制权！问题的严重性不言而喻。

对于用户来说，微软 Office 的最大弊端是与 Windows 紧紧捆绑在一起，它不能在 Linux 等开源软件平台上运行，也没有多厂家的支持。由于历史的原因，微软的 Office 几乎垄断了我国办公软件市场，大部分人使用微软 Office 处理文档。微软还宣

布，从 2008 年起将全面推广 Office 2007，国内用户又将面临一次版式本升级的浪潮。微软 Office 的最大弊端之一是其不同时期的 word 版本（如 1997、2000、2003、2007 版）做不到“精确兼容”，尤其是自 Office 2007 版本起，微软放弃了原有文档存储格式，新老版本文档格式兼容问题更加突出。不仅低版本的 Office 不支持高版本的文档格式，用现在的版本打开 10 年前的 Word 文件也会出错。我军信息化建设中就曾遇到这样的问题，上世纪建成的数据库、文件库、文电库中，有不同时期不同版本 Word 编写的文档，用时下流行的 Windows XP 和 Word 2003 去读，常常会出现莫名其妙的乱码，甚至打不开。某工程为了保证应用程序的兼容，在 2007 年不得不规定各单位要用 word 2000 的版本提交文本。可以设想一下，再过 10 或 20 年，为打开这些文档，我们到何处去找对应的版本？鉴于文档拥有者和使用者都可能无法打开或修改，因此，沿用.doc 格式保存历史文献资料是不安全的，这方面是有深刻历史教训的。PowerPoint 和 Excel 的新老版本中也有类似的不兼容问题。更重要的是，微软的私有格式中可能包括不知情的若干秘密信息，这对政府、军队等要害信息部门是一很大的安全隐患。此外，由于格式不公开，word 中可能含有不良软件，特别是宏病毒与正常的宏指令难以区分，会危及到信息系统的安全。这从反面进一步说明了开放文档格式对于文件电子版存放方式的重要性。

文档格式向我军数据工程建设提出了一个不可忽视的紧迫课题。我军绝大多数办公文档采用封闭.doc 的格式保存，本意是同时保存文档的内容和格式，但由于我们无法通过合法途径获得文档格式的完整、准确的描述信息，所以一旦格式发生变化，就会危及内容的安全。从这个意义上讲，用.doc 保存文档还不如用无格式的纯文本文件.txt 来得可靠，后者内存开销也要低很多。可以说，封闭文档格式已成为办公信息资源共享的障碍，严重影响了国家和军队信息化建设的进程。虽然国产办公软件对.doc 的兼容性已经做得很出色了，但即使这样也不可能做到 100%，而用户对这方面的要求是极为苛刻的。目前，不但国际厂商的办公软件产品文档格式不统一，国内软件厂商之间也缺乏统一标准，这就造成不同办公软件形成的文档无法交流。我国“标文通”标准的诞生，将会加强中文办公软件间的兼容性，对于保障各类政府电子公文和办公文档的长期有效、促进电子政务中的中文办公

软件集成具有重要意义。

### 3 支持国标

UOF 和 ODF 格式最大的优势就在于其开放性和继承性。基于开放格式的文档具有自定义、自解释功能,应用程序通过式样引用可以定义文档的格式,使用通用网络对象(UNO)等先进技术可以保证同一软件不同版本之间的兼容,各级政府所保存的电子文档,在多年以后仍可用任意一款办公软件打开。UOF 和 ODF 支持文档格式与文档内容的分离,可以让不同的办公软件和应用平台自由地交换文件,而不需要理会文件是用何种程序产生的。基于开放格式的办公软件含有不良软件的可能性也将大大降低。

UOF 秉承了独立、完整、开放、可拓展的机制,以 ISO 10646(通用编码字符集)为基础,不仅适用于中文的汉字和少数民族文字,也支持国际字符集。因此,我国信息产业部、科技部、发改委都对项目给予了支持。如果中国全面推行自己的文档格式标准,包括微软在内的各厂商在我国销售办公软件时,就必须符合我们国家的 UOF 标准。对国内软件企业来说,要考虑的就不再是兼容性,而是标准的符合度,大家都站在同一个起跑线上,可以在产品功能和价格上开展竞争。从长远来看,开放的文档格式标准不仅有利于推动信息化的发展,也会成为软件产业发展的重要基石。

UOF 和 ODF 这两个格式都包含办公应用所需的基本元素,注重模块的重用,支持同一标准的多种实现。然而,由于关注重点的差异,它们之间仍存在着显著的差别。如 UOF 专注于中文文档处理的功能,而 ODF 功能覆盖面更加广泛。ODF 采用英文标签;UOF 则采用中文作为标签描述语言,通过标签编码可方便地实现不同语言标签的转换。ODF 文档以部件为基础,采用 ZIP 文件规范;UOF 文档采用单一的 XML 文件形式,文件内部按不同模块压缩存储,效率较高。ODF 还没有数字签名功能,还需要在新的版本中加以丰富;UOF 有些新功能也可融进 ODF 的标准里。总之,两个标准都要继续发展完善,还会有后续版本的推出。

由于都是采用 XML 作为标准描述语言,最终实现两个标准的兼容和融合是完全可能的。因此从宏观上说,支持国标 UFO 就是遵循国际标准 ODF,两者的目标是一致的。为此有如下建议。

#### (1) 统一认识,加强对 UOF 的宣贯力度

应该组织多种形式的宣传和培训活动,让政府、企业和个人都意识到,在国家信息化建设和电子政务工程建设中,采用我国自主创新的文档格式标准,使用国产字处理软件,不完全是技术上的考虑,而且是国家信息产业发展的一项战略抉择,是国家信息安全的需要。教育要先行,建议在高等院校和计算机普及教育中,安排基于开放标准的办公软件的课程。在可能的情况下,应该在国家计算机等级考试、军队专业技术职称考试中,增加国产办公软件操作方法的内容。通过宣传和培训,改变公众对国产办公软件的“惯性思维”认识,逐步熟悉和习惯国产办公软件。

#### (2) 制定相应的采购政策和保障措施

建议在政府集中采购的项目中,优先选择国产办公软件,免费分发给政府机关和企事业单位使用。军队可规定:从 2008 年起,所有型号研制项目中软件文档必须兼容 UOF 格式(有“另存为”UOF 的功能);从现在起到 2010 年止,所有军用文档均应过渡到用 UOF 格式存储。在产品采购时,要强调国产办公软件对用户的技术支持和售后服务。政府还应该打击办公软件领域的盗版行为,保护知识产权,为国内软件企业创造一个公平的竞争环境。

#### (3) 研究已存文档的过渡政策和措施

作为数据工程的一项基本原则,信息的生产者有定期维护信息、实施数据保鲜之责任。目前,军内的图书馆、资料室、档案室等单位存储的电子文档格式繁多,很多电子文件已经找不到相应的软件来打开。因此,需要研制一套功能齐全的文档格式转换工具,能够将众多已归档的文件转换为 UOF 格式保存。有了这种转换工具后,就可以对全军范围内的电子文献进行一次全面的清理,保证政府公文、历史文献的长期有效。

### 参考文献

- [1] 雷赫. 文档格式为谁而争. 中国计算机用户, 第 31 期, 2007.8; 15-16
- [2] 李越. 文档标准: 一场关于开放和垄断的竞争. 科技日报, 2007.8.28; 5

### 作者联系方式

通信地址: 北京丰台区大成路 13 号      邮政编码: 100039      联系电话: 010-66820017

# 部队信息资源开发利用情况研究

潘学俊

**摘 要：**针对当前部队普遍存在的信息资源缺、共享难、利用率低和安全隐患多等问题，作为各级部队来讲，要从应用的角度，围绕统一军事信息系统开发的技术体制和标准、加强现有信息资源存储和管理，提高信息资源的利用效率等三个方面，紧紧围绕部队需求，依靠科学的方法，通过广泛的信息资源采集、有序的信息资源挖掘和优化再生等手段，全面提高信息资源开发利用能力，推进部队信息化建设又好又快地发展。

**关键词：**信息资源；开发利用；部队信息化

随着信息技术的飞速发展和信息主导力的日益增长，信息资源已成为与自然资源、人力资源同等重要的战略资源，其价值已经超出了传统信息的意义。对部队而言，信息资源是战斗力的重要组成部分，是建设信息化军队、打赢信息化战争的重要支撑点。本文主要从当前部队信息资源开发利用的现状入手，研究对策、探索方法，以最大限度挖掘现有信息资源的潜力。

## 1 信息资源开发利用情况的现状和问题

在中国特色军事变革的有力推动下，部队信息化建设进入了持续发展阶段，信息资源开发利用工作也得到了各级的高度重视，各项工作已经起步并初见成效。主要表现在三个方面：一是对信息资源开发利用的地位作用有了充分认识，二是各类数据库建设初具规模，三是信息资源开发利用的标准法规建设全面起步。

同时，还要看到，部队信息资源开发利用工作才刚刚起步，还存在着制约发展的问题，归纳起来有四个方面：

### 1.1 信息资源缺

当前部队信息资源开发利用中最突出的问题，就是各级“重硬轻软”、“重建轻用”、“重系统轻数据”等模糊认识还没有从根本上改变，导致开发建设的野战指挥系统、作战指挥中心、信息网络等硬件档次越来越高，而应用系统没有跟上，效能得不

到充分发挥，使信息资源开发利用没有依托。一些单位舍得投入搞建设，但不愿花钱抓应用，个别甚至还在搞那些所谓的“面子工程”、“观摩工程”，许多单位建成信息系统框架，但没有人搞数据维护、数据更新。重复建设、烟囱林立的现象还没有得到有效遏制，资源浪费比较严重。由于有限的经费都用在了硬件建设上，使得各级在信息资源开发利用上的投入不足，带来的基础信息缺、实时信息缺、频谱数据缺和共享数据缺等问题十分突出。

### 1.2 信息共享难

受当前信息化机制体制的制约，信息资源开发利用总体上还处于自发性、区域性和不规范的状态，主要原因有三个：一是从上至下、上下结合进行统一筹划不够，二是从发展战略与当前任务结合上进行总体设计不够，三是从标准建设到贯彻执行上研究不够。这三个主要原因，客观上造成了信息资源的标准滞后、开发利用各自为政、条块分割、致命“信息孤岛”现象严重，信息资源无法共享。同时，由于存在系统与系统、单位与单位、部门与部门之间的利益冲突，有的部门和单位大搞信息封锁，很多本应该向外开放的信息被据为私有财产，造成信息资源的闲置和浪费。

### 1.3 信息利用低

目前，无论是覆盖全军的信息网络，还是各单位根据自己需求建立的信息网络，真正具有权威性、实用性、规模化的信息和数据还为数不多，网络中多数是单位工作动态、机构和职能介绍、新闻



报道之类的信息,内容单调,且重复现象严重。一些单位建成的局域网,虽然安装了一些高档次的投影显示设备,但数据应用系统智能化程度不高,信息融合、辅助决策、作战模拟功能很弱,面向部队、贴近应用的系统很少,使这些信息网络和系统无法发挥效益。有的单位在系统建设初期没在进行效益评估,没有对部队需求进行论证,结果耗费大量精力和资金开发出来的信息网络和系统,不仅没有丰富信息资源,反而加剧了信息垃圾的泛滥。

## 1.4 安全隐患多

当前部队的信息网络安全保密还不配套,多计算机和局域网设防不严密,计算机芯片、操作系统、高端路由设备等核心技术和产品都是从国外引进的,存在着严重的安全隐患。由于安全管理机制不顺畅,许多单位往往是先搞建设,再加装安全设备,使系统的安全防护存在着先天不足,造成泄密事故频发,严重影响和制约了信息资源开发利用工作的推进。

# 2 信息资源开发利用工作的主要内容

部队信息资源开发利用的目的在于应用,其应用的过程,决不是对信息资源的简单消耗,而是实现信息资源本身的价值,使其增值,再造新的信息资源,促进军用信息资源不断增长的过程,只有这样才能使信息资源开发利用为部队信息化建设提供动力和源泉。

## 2.1 统一系统开发的技术体制和标准

军事信息资源的开发必须在统一的技术体制和标准下进行,这是实现信息资源开发利用有效共享的基础。部队的信息资源从总体上可分为公用信息资源和专用信息资源两大类,公用信息资源是指各级各部门共用的信息资源,如人员、装备等信息,专用信息资源是指仅与一个单位或部门业务相关的信息资源。部队的公用信息资源应统一组织开发、在技术体制、使用软件、模型标准等方面要严格统一,做到标准一致、接口统一,确保公用信息资源真正“共用”。专用信息资源由使用单位组织开发,开发中所使用的技术体制和相应标准也要符合国标、军标的规范要求,能与公用信息资源一致的

要尽量一致,便于两类信息在需要时能有效无障碍地交流使用。特别需要注意的是,在各单位各部门使用的专用信息资源中,都包含有公用信息资源,在开发使用专用信息资源的过程中,各单位各部门要按照公用信息资源的要求来开发和使用,在管理上要列为公用信息资源,以提供给部队的所有用户共用。

## 2.2 做好现有信息资源的存储和管理

信息资源具有可湮没和可流失性,在军事领域,要想获取战场军事信息优势,就必须对现有的信息资源进行有效的存储和管理,只有这样,才能促进军事信息资源量的不断增长。对军事信息资源的存储与管理,主要通过分类建立数据库及信息管理系统的方式来实现。

### 2.2.1 建立信息资源数据库

信息资源数据库是以一定的组织方式将各类信息资源合理地存放在一起,具有数据源多、信息量大、共享面宽、可靠性高、可用性好、易扩充等特点,并可为多种应用提供数据共享服务。由于管理体制和技术方面等一系列的原因,目前大量的信息资源数据库是分散和孤立的,采用了不同型号和不同版本的数据库管理系统,各成体系,无法互联互通。为了解决和实现信息共享和互操作问题,需要将现有的分散异构的信息资源数据库系统连接起来,集成为一个互联、互通、互操作的分布式的联合共享数据库,这就要求必须要统一数据库的建设管理,建立统一规范的系统平台和数据的格式标准。

### 2.2.2 构建信息资源数据仓库

军事信息资源数据仓库是为了解决数据库不能有效支持分析处理典型的问题而发展起来的,主要用于管理大时间跨度的大量历史数据,以便更好地支持作战决策的一种数据管理技术。作为一种数据管理技术,它将分布在不同数据库中的数据,按照统一格式、统一数据结构和编码、围绕不同的主题,以集成重组和存储的方式,以方便用户对信息的访问,使决策人员能对较长时间内的历史数据进行分析,发现有用的知识或规律,从而确定建设的未来发展趋势。

## 2.3 全面提高信息资源的利用效率

信息资源开发利用中,开发是基础,利用是目的,提高利用效率是做好此项工作的根本出发点和落脚点,主要应该从四个方面入手。

### 2.3.1 努力提高信息资源的共享水平

随着部队信息化水平的不断提高,以及需求研究的不断深入和细化,各种各样的面向不同军事需求的数据库、数据仓库将会大量开发出来。针对军用信息数据库的多样性和分布范围广泛的特点,可以采用超媒体链接技术实现信息资源的互联互通,也是提高部队信息化水平的重要措施。所谓的超媒体技术就是将超文本技术与多媒体技术结合起来,将文字、图表、图像、视频、音频等信息资料以一定的方式相互连接,形成一种非线性的网状结构。这种技术再向数据库延伸,就可以成为超媒体数据库系统。这种技术的应用和系统的建立,可以满足不同使用者对不同信息的需求,有效地利用网络资源和信息资源。

### 2.3.2 努力提高信息技术资源的利用效率

科技进步使信息资源在部队的推广与普及加快,效益增大,如何有效运用这些信息技术成为关键。一是要通过统一通信体制,扩大通信资源运用的空间,充分发挥已有的有线、无线、卫星、光纤和网络通信手段的潜能,增强军事信息的传输能力;二是通过一体化信息系统建设,充分发挥各类传感系统的效能,增强信息获取能力;三是最大限度地将计算机和网络技术应用于指挥系统,提高部队作战指挥能力和实际对抗能力。

### 2.3.3 努力提高动态信息资源的利用时效

战场动态信息资源利用是信息资源利用的重点和难点,要实现对这一资源的有效利用,就必须从信息获取、使用、防护三个方面入手。一是要明确需求,对所需信息的种类、数量非常清楚,才能有的放矢,合理区分力量进行获取。二是适时利用信息。在实际作战行动中,对所有信息环境和信息系统,无论是己方的还是敌方的,也无论是军事的还是非军事的,如有可能都要加以利用,以增强对战场的控制能力。三是要注重信息防护。战争实践证明,对武器系统所信赖的信息或信息系统实施重点打击,扰乱对方指挥与控制系统,破坏其作战情报

资源的共享和分配环境,是最有效的攻击手段。因此,在作战中必须要充分地考虑己方信息系统的薄弱环节,采取科学的防范措施,以提高信息系统资源防护能力。

### 2.3.4 努力构建科学合理的信息资源配置机制

军用信息资源的价值在一定程度上体现在其时效性上,有的信息可以被部队长期利用,有的则只用于某一段时间,因此这些对部队行动产生重要影响的军用信息资源呈现出随机性。由于战场信息资源数量巨大、类型丰富,为提高其使用效益,必须建立高效的军用信息资源配置机制。一是改进信息资源配置方式,按需调配,减少信息资源闲置,提高军用信息资源利用率。二是逐步形成以技术促信息资源开发,以信息技术开发促技术进步的良性循环机制,以此来促进军用信息资源的快速增长,促进军队信息资源利用向实时化方向发展。

## 3 组织开展信息资源开发利用的有效对策

由于信息资源开发利用工作在信息化建设中地位的不断提升,各级逐步加大对信息资源开发利用的重视程度,加大投入、重点建设。在部队中信息资源开发利用是提高军用资源数、质量的关键环节,必须紧紧围绕部队需求,依靠科学的方法,通过信息的采集、挖掘、资源优化和信息再生几个环节进行有序的进行。

### 3.1 广泛的信息资源采集

信息资源是无限的,而信息采集能力是有限的。结合军事需求,信息资源的采集,必须要具有很强的目的性,围绕与军事行动紧密相关的需求,通过资料收集、实地勘测、信息测智、分析整理等手段,采集那些真实的、有实用价值的、能反映部队建设发展本质规律的信息,以提高所采集信息的有序性、系统性和实用性。要明确系统采集的内容和主体,各个单位部门要结合任务区分采集内容。要灵活运用系统采集的方式方法,发挥各种采集手段的综合效能,多方位、多视角、实时地采取所需要的信息。要构建多元化的信息采集体系,对战场的各种目标信息、战场态势信息、战场变化信息进

行实时采集,同时,及时了解国内外军事动态和外军信息化建设的发展动向,为部队信息化建设提供信息支持,为作战行动提供信息保障。

### 3.2 科学有序的信息资源挖掘

有序的资源挖掘可以从数据和信息资源挖掘两个方面来理解。人们常说的数据挖掘,是指从大量的、不完全的、有噪声的、模糊的、随机的数据中,提取隐含在其中的、人们事先不知道的,但又是潜在有用的信息和知识的过程。其实质是和各种分析工具在海量数据中发现模式和数据间关系,并对此进行描述和预测。信息挖掘是一种用于开发信息资源的新的深层次数据处理技术。它基于人工智能技术、统计学等先进科学,能够高度自动化地对大量数据进行归纳推理,从中挖掘出隐含的、先前未被发现的、对决策有潜在价值的知识和规则,是一种高级信息处理过程和决策支持过程。随着信息技术的不断进步,数据库和数据仓库的容量越来越大,但若没有高效的数据分析和挖掘工具,要寻找隐蔽在其中的有用信息十分困难。再完善的数据库、数据仓库都将变成无用之库。信息挖掘技术就是在这种需求下产生的,它的研究和开发,需要涉及多个知识领域,包括数据库技术、人工智能、神经网络、统计科学、模式识别、知识获取技术、信息索引技术、高性能计算技术等,其主要任务是从海量数据中发现模式,并通过预测型模式和描述型模式来描述数据集中的特性。

### 3.3 信息资源的融合与再生

信息资源融合与再生,是指采集的客观信息与

**参考文献(略)**

#### 作者联系方式

通信地址:沈阳市和平区太原北街5号18组

邮政编码:110001

联系电话:024-23082812

人的主观思维有机融合生产新信息的过程。但只有采用科学的技术及方法,才能实现高质量的信息再生。

#### 3.3.1 优选信息资源

军事信息资源的优选重在鉴别。即纵向要比历史,了解部队在不同时期的建设状态,找出适合部队特点的信息化建设规律;横向要比同类,掌握同等条件下部队的信息化建设差异,找出问题原因。同时,面对浩如烟海的军事信息,要注意抓大放小,对事关部队信息化建设大局、关系部队全面发展的重要信息,一定要抓紧抓牢,彻底弄清弄准;对一般要定性鉴别,尽可能地进行定量分析,不要被“垃圾”信息所迷惑,浪费过多精力而无用。

#### 3.3.2 消除信息资源的不确定性

主要是应该加强部队的需求研究,使部队各项活动的透明度不断提高,从而理清和减少部队需求研究中的不定、未知、疑义和混杂的因素,找出部队信息化建设中的主要矛盾,消除模糊认识,更好地把握部队信息化建设方向。

#### 3.3.2 进行信息资源的融合与再生

要充分利用人工智能技术,按照一定准则,把从不同渠道、不同层次获取的信息资源进行互联、估计及组合等多层次、多方面的自动分析和综合处理,获得准确的结论性信息,完整而及时地对部队信息化建设和战场态势进行评估,从而完成所需新信息的再生,为部队建设和军事行动提供更加科学的依据。

# 地面防空指挥自动化系统研究分析

徐榕 牟东

**摘 要:** 首先分析了建设地面防空指挥自动化系统的重要意义, 然后详细介绍了地面防空指挥自动化系统的指标, 接着分析了系统的建设重点和主要功能, 最后给出了防空探测系统建设的技术改造方法。

**关键词:** 地面防空; 指挥自动化系统; 对策研究

近几场局部战争表明, 在信息化条件下的局部战争, 都是以空袭与反空袭的作战行动贯穿局部战争全进程的主要作战样式。而在空袭与反空袭的作战行动中, 在空袭进攻中, 广泛使用隐形、远射、精导等高技术兵器又是其主要特征。由于这些兵器具有精度高、威力大、投射距离远、对目标的选择性强、机动范围大的特点。这就对地面防空作战指挥自动化系统提出了更高的要求。

因此, 加强我军地面防空指挥自动化系统的研究, 将是系统建设前需要重点研究课题之一。

## 1 指标分析

由于未来反空袭作战中, 我军的主要对手具有综合技术优势, 较易达成对我空袭行动的突然性。这就要求防空战术单位应具有: 实时、严密地掌握空情, 准确、快速地分析判断情况, 及时、正确地定下运用火力的决心, 精确、有效地组织下级作战的能力。这些能力的有效性的体现, 通常都是在短暂时限内完成的。要达到这一点, 防空战术单位指挥自动化系统必须实现以下基本要求:

### (1) 时效精度高

防空作战指挥的时效性主要由情报、决策、通信和武器系统的最短准备时间的时效性等人、机系统综合时效构成, 精度则主要指系统误差小。

1) 在空情处理方面。空情录取、识别、传递、接收、处理和显示等环节必须实现自动化或半自动化, 以缩短时间, 减小误差, 保证给指挥员提供及时、连续、可靠的空情信息, 满足武器系统的预警时间和对空射击要求。主要内容有: 空情信息保障空域, 处理目标范围, 处理精度与时延等。

2) 在辅助决策方面。系统实现飞行诸元和射

击诸元自动计算(包括目标飞行速度、高度, 航路捷径, 到达火力范围时间, 批次间隔, 武器系统指向等); 适时显示防区的空情, 包括目标航迹, 飞行诸元, 对不同信息来源能相互转换、综合处理; 根据预先设置的准则、数据, 自动判定目标的威胁程度; 适时向指挥员提供任务区分, 指挥程序提示, 组织运用火力的决心建议(含火力分配计划)。提供火力配系、电磁态势、部队人员与装备的状态等信息。

3) 在通信保障方面。快速、可靠、保密是对信息传输网络和手段的基本要求。具体来讲, 通信信道应保证数/话双向双工通信, 既要保障空情数据传输的及时性、可靠性, 又要保障不间断地对所属进行指挥控制。既能保障指挥员实施逐级指挥, 也可实施越级指挥。为提高时效性, 空情信息传递(含部队突然发现、上报的预警空情信息)。

### (2) 环境适应强

这主要体现在三个方面: 一是在系统工作环境指标上, 应以系统可能运用的环境的最坏条件为指标, 如沿海的潮湿、盐雾、高温、抗精确制导武器打击等; 系统最低作战保障性能等(如: 在自动化、半自动化和人工三种工作状态的顺畅转换等)。二是系统在适应要地防空与机动作战的要求上, 应向适用于机动作战方面靠拢; 三是在指挥模式上, 系统应体现训、战结合, 具有作战、战备值班和模拟训练三种模式。

### (3) 系统容量大

系统容量主要包括指挥、情报、传输、存储等容量。

指挥容量: 应满足防空战术单位对所属单元和友邻部队的指挥控制需要。

情报容量: 一是指系统空情信息来源的数量,

通常是根据所属情报的数量决定,防空战术单位直接获取的空情通常应经融合后传至上级,必要时可越级发送。二是指系统接收处理和综合处理输出空情的数量。这又分为近空空情与远空空情,接收处理近空空情的数量应大于武器系统的最大火力打击能力的上限,远空空情为综合处理输出,应为本防卫区的重点批空情的数量。

**传输容量:**主要是指满足传输数据和指挥控制需要的信道带宽。

**存储容量:**主要是指空情数据存储量,作战数据库中存储的文字、数据的大小。

#### (4) 可靠性高

主要指系统设备连续工作时间(系统设备连续工作时间应按现代空袭战役最长时间作为参考系进行设计)、自动监测、故障判断定位,重构(系统重构应按模块化设计要求)、扩充能力、系统最低作战保障性能等。

#### (5) 顽存性好

主要是指系统在战时的生存度指标,如防空探测系统被敌发现、摧毁的概率大小,指控系统抗敌打击的能力强弱等。

## 2 防空指挥自动化系统建设重点

防空指挥自动化系统建设的目的是提高防空部队的空中态势共享能力、快速反应能力、机动作战能力、军(兵)种协同能力、生存和保障能力,从而实现防空体系的一体化。因此,系统建设重点主要体现在五个方面:一是多方式、多路由的通信组网,保障防空指挥控制系统的互联互通,实现空情处理、作战指挥的网络化。二是充分而有效地利用各种情报源,提高目标发现概率;三是辅助制定作战计划,提高科学决策的水平,缩短作战准备时间;四是防空指挥控制系统对隶属和加强的防空部队实施高效的作战指挥;五是对高炮、地空导弹等防空武器实施自动化的射击指挥和有效的控制。

## 3 指控系统的主要功能

系统功能主要有:预警探测、空情处理、战场态势、辅助决策、作战指挥、模拟训练等六个方面。

### 3.1 预警探测情报

预警探测情报包括:所属上报的雷达空情、火控空情、侦察信息、上级通报空情信息等空域动态情报。

### 3.2 空情处理

空情处理主要有:对空情进行接收、数据融合等处理,计算、显示目标航迹与参数,进行威胁估计、排序和相关计算,对空情目标进行人工、自动消批,改、合、分批等处理功能。

### 3.3 战场态势

实时、高效、准确的战场态势是指挥员对所辖兵力进行指挥、控制和协调的基础,是指挥员优化火力运用,提高对空抗击能力的基本条件之一。它是系统与指挥员交互的主要界面。

### 3.4 辅助决策

#### (1) 辅助分析

1) 生成方案:根据总的作战任务,上级作战意图,作战方式,作战地域的水文、气象、地理条件,保卫目标的特性及价值,所辖兵力的大小及武器系统性能,作战条令和军事规则,专家规则和效果评估等因素,以一定的人机交互方式,系统辅助生成兵力部署方案、侦察配系方案、协同方案、火力分配方案、电子对抗方案等;辅助指挥人员生成表格或图示方案、生成相应的作战文书;在作战过程中进行目标威胁度分析评估,根据武器性能、战场环境变化,辅助指挥人员及时生成实时生成火力分配和火力协调方案,兵力部署调整方案。

2) 系统重演。它是记录作战过程,进行作战分析,提供区分责任数据的必备手段,应对作战主要指挥要素、战位进行录音、录像,系统提供按作战进程打印航迹图、战况数据及作战文书等重演功能。

#### (2) 方案管理

对作战方案进行调阅、拷贝、输出、删除、修改等管理操作。

### 3.5 作战指挥

作战指挥功能主要包括四个方面。

1) 指控:接受上级指挥所的指挥,对所属及

临时配属和加强的各作战单位进行直接或越级作战指挥；进行实时任务分配和火力区分；对所属防空兵力下达射击命令，进行目标指示和目标校对，实现对火控系统的自动引导；与航空兵协同时，明确记录协同数据，并向所属部队明确注意事项；与友邻防空部队协同时，对下级发出协同指示；自动进行敌航空器的威胁判断，以人机交互方式形成综合对空防御方案，组织部队进行对空防御；动态分配侦察力量；

2) 作业：作业包括文电、图形、和数据库三个主要内容。

3) 警报。当敌目标临近、进入我目标防卫区域时，系统能可靠地发布预警、告警。

4) 通信。与上级、下级、目标指示雷达站、哨所站、友邻防空部队和被掩护部队等保持话音、数据通信，及空中截击力量的协同通信；

### 3.6 模拟训练

为利于平时实施系统仿真模拟训练，系统产生模拟空情数据的方式进行训练，模拟训练产生的数据、报文、话音等应与作战数据能够自动区分、存储、调阅。

## 4 防空探测系统建设

在高技术局部战争中，信息进攻武器对探测系统的生存构成了严重威胁，提高探测系统有效性和顽存性，已成为夺取反空袭作战的胜利的必要条件之一。因此，除了加强防空指挥自动化系统建设

参考文献（略）

### 作者联系方式

通信地址：广州达道路2号大院13号

邮政编码：510600

联系电话：020—87171380

外，还必须对探测系统进行技术改造。

1) 采用多技术体制雷达组合，装备具有多体制的雷达系统，提高系统有效性和顽存性。由于反辐射导弹受载荷、容积和信号接收机和天线的频宽等技术限制，其难以制作适应全性能要求的接收天线和接收机，因此在雷达探测系统中，合理地发展、部署多体制雷达，地面制导雷达和合适的炮瞄雷达，可有效增加反辐射导弹制作难度。同时，在现代高技术战场上，通过及时改变雷达工作技术参数，减小雷达信号的强度等技术体制，来增加反辐射导弹导引头选择器选择和锁定难度，从而干扰反辐射导弹的攻击的锁定概率和准确性，也是十分有效地抗导弹攻击的技术方法。

2) 从技术手段上提高系统探测和生存能力。充分运用上级的提供预先情报，增加其它无源探测系统，减少、减短雷达开机时间，提高雷达生存概率，提高掌握隐形战机的活动情况的能力。

建立地面防空系统与空中等探测系统的通信系统，提高预警时间和减少地面雷达系统的开机时间，解决地面雷达的低空探测盲区和有效延伸探测距离的问题，提高地面雷达探测系统的生存能力。

3) 从系统结构上提高雷达网整体探测效能和生存能力。为弥补单一雷达生存能力弱、探测能力和探测精度低的弱点，指挥自动化系统应将各种雷达传感器联接成网络，实现对雷达探测信息数据进行融合和对各雷达灵活有效的控管。或采用灵活的配置的方法。从系统结构上提高雷达网整体探测效能和生存能力。

# 加强指挥信息系统建设与运用的几点思考

柳晓宏 山峰 范雄飞

**摘 要：**本文结合我军信息化建设发展形势，从理论创新、体系建设、检验评估、系统训练、频谱管控等方面，对指挥信息系统建设和运用进行了理论探讨。

**关键词：**指挥信息系统；建设

指挥信息系统是各级指挥员实施作战指挥的平台，是实施联合作战的物质基础，更是联合作战指挥体系的关键要素和军队信息化建设的核心内容。随着信息化建设和军事斗争准备的深入发展，如何解决好“建”与“用”的关系，真正发挥好指挥信息系统在信息化条件下战争中“粘合剂”和战斗力“倍增器”的作用，实现信息力与火力的有机铰链，全面形成部队信息化体系作战能力，是摆在我们面前的现实课题。

## 1 结合部队发展和未来战争需要，以理论先导牵引系统建设和组织运用的创新发展

创新是贯彻落实科学发展观的内在要求，也是推动部队建设发展的不竭动力。我军指挥信息系统建设要以科学发展观为指导，进一步增强理论研究的战略性、前瞻性和针对性。一是超前预想，科学谋划。要以需求为牵引，紧密结合军事斗争准备各项任务，按照信息化建设顶层规划的统一部署，及时总结梳理现阶段建设成果，进一步论证预测信息化体系作战能力对指挥信息系统的建设需求，细化落实各项规划计划的具体措施，为筹划下一阶段建设任务奠定基础。二是运用现代科学理论，加强建设与管理。针对新装备作战保障能力的形成，将系统论、信息论、控制论、人机工程理论引入指挥信息系统建设，改进装备建设管理保障模式；采用生命结构法、原型法、渐进获取法等基本方法，对系统装备研制生产实施周期管理、性能管理、安全管理和智能控制，确保指挥信息系统装备建设与管理效益最大化。三是立足实战，完善作战理论。随着指挥信息系统技术水平的不断提高，应重点深化指挥信息系统在信息化条件下作战的组织运用研究，

积极探索新时期指挥信息系统装备建设和作战运用的特点规律，从战术和技术上形成可行、可靠的保障方（预）案，为战时系统效能的发挥提供可靠依据。

## 2 以形成体系能力为出发点，着力强化综合集成建设

要实现我军“建设信息化军队，打赢信息化战争”的战略目标，必须将全面提高体系作战能力放在突出位置统筹安排，运用综合集成的建设方法，加强指挥信息系统各要素间的融合。一是进一步加强一体化设计。以统一技术体制为切入点，采用先进成熟技术，完善各级各类指挥系统，并以此带动和促进相关业务领域的一体化建设与发展，加大各分系统、各要素与指挥控制系统的同步设计、同步建设、同步配套力度，确保同步形成能力。二是加强系统间的紧密铰链。深入研究数据交换格式、通信协议、传输方式、以及主要战术技术性能等通用性要求，有效解决系统间信息交换的标准化问题，提高系统接口标准化水平，不断提高对武器装备和部队的精确控制能力。围绕军事信息的采集、传输、处理和分发各个环节，以指挥信息系统为核心，以信息高效整合和流动为出发点，逐步形成军事信息闭环链路，为部队形成体系作战能力提供一体化的指挥保障和技术支撑平台。三是加强信息对抗能力建设。以信息安全保护为关键环节，在新型指挥信息系统装备的研制阶段，将抗干扰技术应用突出出来，从技术上研究抗干扰手段措施，优化战技性能指标，着力构建系统配套、攻防兼备、平战结合、多层次、多手段的综合信息防护体系，满足部队全域运用、多方向作战的需要。

### 3 以满足部队使用需要为标准, 严格指挥信息系统效能检验评估

效能检验评估是保证装备质量建设的基本手段, 是科学管理的内在要求, 也是对信息系统进行全程、全寿命闭环质量管控体系的重要环节。指挥信息系统装备在交付部队使用之前, 要经过严格的测试检验和检查验收, 确保装备各项性能满足战术技术指标要求和部队作战需要。为此, 一是加强系统效能检验规划设计与协调。对指挥信息系统装备复杂战场环境条件下全流程、全要素效能检验, 以及武器装备配套性检验实施统筹规划, 科学设计, 周密协调, 合理调配各方面力量, 确保实效。二是研究制定系统测评指标体系和能力评估标准。根据信息技术的发展和作战需求的变化, 依据国家军队有关标准, 结合部队信息化建设实际, 按照先进、准确、可操作的要求, 制定信息系统测评指标体系和能力评估标准, 为系统验收和检查评估提供权威、统一、可靠的科学依据。三是不断完善检验评估手段。在充分利用和进一步完善我军已建试验场所的同时, 逐步加强与军兵种武器装备发展相适应的检验环境建设, 进一步提高信息化作战条件下系统效能检验能力, 同时也可部队训练提供场所和手段。四是研究建立检查评估机制。从制度机制上建立完善责任体系, 实行责任制, 认真研究加强行政指挥和技术指挥的措施办法, 行政指挥和技术指挥两条指挥线密切配合、高度协同, 不断提高系统检验评估水平。

### 4 着眼人与装备的有机结合, 重点加强部队在复杂环境条件下指挥通信训练

复杂电磁环境是信息化条件下作战的显著特征。开展信息化战场环境尤其是复杂电磁环境条件下的练兵, 是推进部队现代化建设向信息化作战能力转化的重要切入点。因此, 要充分发挥军事训练的抓手作用, 切实把加强指挥信息系统装备在复杂电磁环境下的组织运用突出出来。一是拓宽训练领域, 拓展训练内容, 增强训练的针对性。着力抓好部队在复杂电磁环境下的实战化、一体化训练研究, 加大联合训练力度, 组织指挥信息系统全过

程、全要素对抗演练, 以及抗扰、抗毁战术技术训练, 研练单台抗扰、网络抗毁、体系对抗的有效对策, 综合提高部队对抗作战能力。二是创新训练方法, 提高训练的实际效能。深入研究探索信息化条件下作战部队训练特点规律, 改革传统的训练模式, 建立和完善适应信息化作战的训练理论和训练体系。根据信息化装备的发展和部队承担的作战任务, 完善训练大纲, 建立健全法规制度, 强化训练效果的检验验证和考核评估。三是创新训练手段, 完善训练场区配套设施建设, 构建近似实战的训练环境。围绕信息化条件下部队训练模式转变, 通过不断提高军事训练的科技含量, 统一调配训练资源, 着力构建一体化军事训练网系; 充分利用模拟仿真技术, 加强复杂电磁环境评价体系和建模研究, 建立科学、合理、客观的评价模型, 为复杂电磁环境下指挥信息系统组织应用提供基础; 研究开发信息化作战模拟环境, 为开展对抗训练创造条件。通过训练检验武器装备性能, 促进人才培养, 牵引编制体制调整和武器装备发展, 促进部队信息化作战、综合保障能力的快速提升。

### 5 力争先机夺取电磁优势, 加强战场电磁频谱管控力度

随着武器装备信息技术含量的加大, 用频装备已嵌入多种武器装备平台, 电磁频谱管控与部队的战斗力和战场生存能力密切相关。科学而有效地实施战场电磁频谱管控, 优化我方电磁环境, 力争夺取制电磁权, 是抗击敌方电磁攻击, 确保我方指挥信息系统战时效能发挥和克敌制胜的前提和关键。为此, 一是加强电磁频谱管控技术手段研究。深入分析研究未来战场电磁频谱管控的特点和需求, 搞好顶层设计, 指导电磁频谱管控手段建设, 提高电磁频谱管控能力, 实现用频武器装备部署合理、战场电磁环境实时监测、干扰源快速定位和电磁态势准确分析, 同时要加强对武器装备系统应对电磁干扰的防护研究, 提出电磁防护的具体标准, 做到电磁频谱管控有据可依, 满足部队作战对电磁频谱管控的需要。二是摸清战场电磁环境。加紧对敌用频装备、侦察干扰装备和组织运用方式的研究, 形成切实可行的对策, 提高自身防护能力。同时, 准确掌握我用频装备间的自扰、互扰, 根据指挥通信装备战技术性能、部署区域, 区分不同手段, 区分民



用、友邻和自用，通过对环境构建效果的评估，摸清通指装备自扰互扰的“底数”，做到知己知彼。三是完善电磁频谱管控工作秩序。加强用频装备整体筹划和综合管控，形成充分协商，科学指配，高效运行的电磁频谱管控工作机制；论证管控网系构建框架，确立指挥体制，明确管控机构编成、职能及任务，确定装备选型配置方案，确保频谱资源的有效利用。

## 6 指挥信息系统组织运用应把握的几点原则

一是周密计划，充分准备。紧贴军事斗争准备需求，坚持从最困难、最复杂的情况出发，科学制订指挥信息系统保障方案。合理编组作战保障力量，科学安排预备力量，确保战时保障力量的合理运用、快速补充和信息能力的快速恢复。二是全面组织，确保重点。从作战全局出发，对各级各类指挥信息系统统一组织，全面规划，建立纵横相连、衔接关照、相互补充的保障体系。要把保障的

重心放在确保对作战行动具有决定性影响的主要方向、重点部队和作战的关节点上，力争战时形成局部信息优势，确保作战指挥的稳定可靠。三是军地兼用，机固结合。以各级各类指挥信息系统为重点，以地方通信资源为重要补充，形成点线一体、机固融合、梯次配置的保障能力，确保在复杂战场环境下指挥通信全时畅通。四是严密防护，严格保密。针对敌方可能的攻击破坏手段，加强对指挥信息系统设施的综合防护和警戒防卫，并从反侦察、反干扰以及防电磁脉冲和计算机病毒等方面采取防护措施，以抗击敌人的“软”、“硬”打击；从指挥、管理和技术等方面采取有效措施，严格遵守保密制度，灵活采取多种保密手段和措施，确保信息安全。五是严格管理，整体协调。建立完善的指挥管理体系，运用科学、严格的管理措施，对作战指挥行动实施统一的指挥控制，使系统内各要素、各方向密切配合，形成良好的运行秩序。实施强有力不间断的整体协调，使各级指挥信息保障力量形成一个有机结合的整体，从而提高信息系统的整体保障能力。

参考文献（略）

作者联系方式

通信地址：北京市海淀区清河大楼甲3号

邮政编码：100085

联系电话：010-66335928      13520149975

# 武警森林部队战术机动综合信息系统构建与应用研究

聂坤华

**摘要：**武警森林部队是一支以防火灭火为中心，保护国家森林资源的专业武装力量，是扑救森林火灾的突击队和主力军。本文分析了武警森林部队当前通信手段存在的不足，提出了建设“战术机动综合信息系统”的构想，为构建武警森林部队战术机动综合指挥平台提供思路。

**关键词：**战术机动；信息系统

## 1 武警森林部队战术机动综合信息系统建设需求

武警森林部队是一支以防火灭火为中心，保护国家森林资源的专业武装力量，是扑救森林火灾的突击队和主力军。森林部队主要分布在东北、西南、西北等国有重点林区，担负着森林、草原防护任务。作战行动具有区域广、时间不确定、地形环境复杂等特点，尤其是原始林区山高林密、机动不便、自然条件差。指挥通信无资源可利用，通信联络完全立足自我保障。目前国内外现有通信手段无法满足部队完成任务需要，部队灭火作战通信指挥无法得到可靠保障。部队急需解决：单兵通信与士兵双手作业的矛盾；火灾现场指挥通信困难问题；现有各种通信手段的互联互通；数模通信兼容的问题等。以确保各级指挥员能随时指挥控制部队，实现语音、数据、图像综合应用。

森林部队灭火作战，基本组成以班排（架次），中队（连）、大队（营）、支队（团）和总队（师）为单位，根据火场态势，参战单位从一个架次到若干支队乃至跨省以上的总队联合作战不等，参战区域从数百平方公里到千余平方公里，还需要与解放军、武警其他部队、地方专业灭火队等单位建立协同通信。为此，部队指挥通信任务异常艰巨，急需研究解决：一是完善单兵通信；二是健全火灾现场通信；三是实现远、中、近距离及现有各种通信手段的互联互通；四是解决模拟通信与数字通信兼容的问题。

综上所述，根据部队作战特点及通信建设现状，充分利用国内外民用通信技术创新成果，构建以超短波为基础，以智能控制软件技术为支撑，融无线通信、有线通信、卫星通信、计算机网络通信

为一体，实现语音、数据、图像综合应用的战术机动综合信息系统，才能满足部队机动灭火作战指挥需要。

## 2 武警森林部队战术机动综合信息系统设计构想

森林部队战术机动综合信息系统建设，主要解决团以下部队机动指挥信息通信问题。系统组成可包括头盔式对讲机（单兵电台），GPS 对讲机（班排长电台），智能一体机（营连长电台），背负式多功能转信台，数字车载台，跨频段多功能指挥调度台，多通道数字基地转信台等部分组成。

### 2.1 单兵电台的设计

主机结构包括：超短波收发机，数传调制解调器、蓝牙和 USB 接口，报警器，智能电源管理。

单兵电台是以 1-5 瓦功率超短波信道机作为主机，内置专业化蓝牙接口、配套头（钢）盔式蓝牙送受话器和可选配的无线 PTT 开关、内嵌数字接口和呼救报警器。将主机挂于腰间，蓝牙送受话器置于各种头盔内，电台通话开关采用无线 PTT，置手指或枪托上。该台解决了单兵作业手持各类器械下的通信问题，本机兼报警呼救和室内定位功能，是实用的单兵通信装备。

### 2.2 GPS对讲机的设计

设计主要包括如下：超短波收发信模块、数传及调制解调模块、GPS 模块，三者通过统一的 MCU 进行控制和管理。

GPS 对讲机是班排长使用手持台，该机功率

1~7 瓦可调,通信距离是常规对讲机 1~1.5 倍,能与地理信息系统联网,电池能超长使用,有 PDA 接口。该机特别适合于林区作战、巡逻执勤或通信距离较远使用。

## 2.3 智能一体机的设计

智能一体机是由 5 瓦超短波收发信模块(含数传)、GSM(CDMA)模块、蓝牙模块、GPS 模块、摄像模块等都是以 PDA(掌上电脑)模块为中心设备,在软硬件上融合成智能化手持终端。

该机可根据不同的任务,启动或联动一个至多个硬件模块和软件模块,完成语音、数据、文件、短信、图片、导航等多种业务。并且在各种进程中相互协调,按照智能化,合理化的模式自动进行软硬件资源调配,解决了各类无线信息终端功能单一、数话分离、互不相联的问题,将各类业务集成在掌上电脑上,还可与指挥自动化网互联,实现移动专网业务功能。

## 2.4 背负式多功能转信台的设计

该台以智能控制器为主体,内置 25 瓦轻型超短波数字化电台、GPS 定位仪、数传电台和 9 种通信协议的自适应接口。

可作为转信台,延长对讲机、车载台等通信距离 20~30 公里;能将超短波、短波电台,移动、有线、卫星电话进行互通,实现远距离数字和话音转信、指挥调度,能与计算机网互联,能实现 GPS 自动导航定位和 GPS 转信定位,图片传输,文件、短信收发;具有 GPS 定位差分、计算机网络节点和多级转信等功能;主要由单兵背负使用。

## 2.5 数字车载台设计

数字车载台主要由 25 瓦超短波收发信模块(含数传)、GPS 模块为中心设备,外接掌上电脑(计算机)。

数字车载台具备语音和数字通信(GPS 定位,图片传输,文件、短信收发等)功能,可与其他野战指挥系统和固定指挥自动化系统互连。是本系统与其他数字系统接入主要设备。

## 2.6 跨频段指挥调度台设计

内置三个不同频段 25 瓦轻型超短波数字化电

台、GPS 定位仪、数传电台和 9 种通信协议的自适应接口,可使同时参加救灾的军、警、民使用不同频段超短波电台互联互通,各频段又可独立工作,并可与现有其他通信手段互通互联。

## 2.7 多通道数字基地转信台设计

本机根据需要将 1 至 3 通道(每个通道可编 99 信道,数话兼容、自动识别)数字化 25~50 瓦功率转信台主机用于野战指挥机构同时多路转信,超短波接力组网,并能转信类型短波、GSM、CDMA、有线、卫星电话,数据类型 GPS、WORD 等各类文件、图片、短信,集带通滤波型双工器和多路天线共用器、同频同播控制板等全系列设备于一体。具有高度集成,小型化、大功率、多路通特点,

# 3 武警森林部队战术机动综合信息系统的技术体制

系统技术体制是提供或者支持作战功能、系统及互联的,它定义关键节点、电路、网络、作战平台的物理连接、位置和标识,规定系统和组成部分的性能参数。

## 3.1 系统标识

系统内所有设备,均应有一套完整的 ID 标识体系,惟一的 ID 号,身份码通过计算机系统动态管理,可以进行无线电遥控开关机。

## 3.2 系统信令

系统的信令,包括频道标识、数据帧格式、纠错格式、文字和命令格式、声码器格式、GIS 信息格式、选呼信令、遥控信令等,它能够保证网内设备可靠互联互通,并且具有保密和抗干扰的功能。

## 3.3 系统接口

系统接口,它是系统空中无线接口和物理接口体系采用的统一标准。空中接口包括超短波信令接口和信号接口、短波信令接口和信号接口、互通互转接口、加密信令接口、图像信令接口、短信信令接口等;物理接口包括标准 RS232 接口、USB 接

口和计算机网络接口、野战电源接口。

4 武警森林部队战术机动综合信息系统的组织应用

武警森林部队战术机动综合信息系统能在野外各种恶劣环境条件下保持良好工作状态，具有灵活

机动的组网和数模兼容功能，实现了从单兵、大（中）队到前线指挥所及预设战场所需要的语音、数据、文件、短信、静态图像、定位等多种业务应用。形成了从单兵到各级指挥员通信装备的系列化。详见图 1。

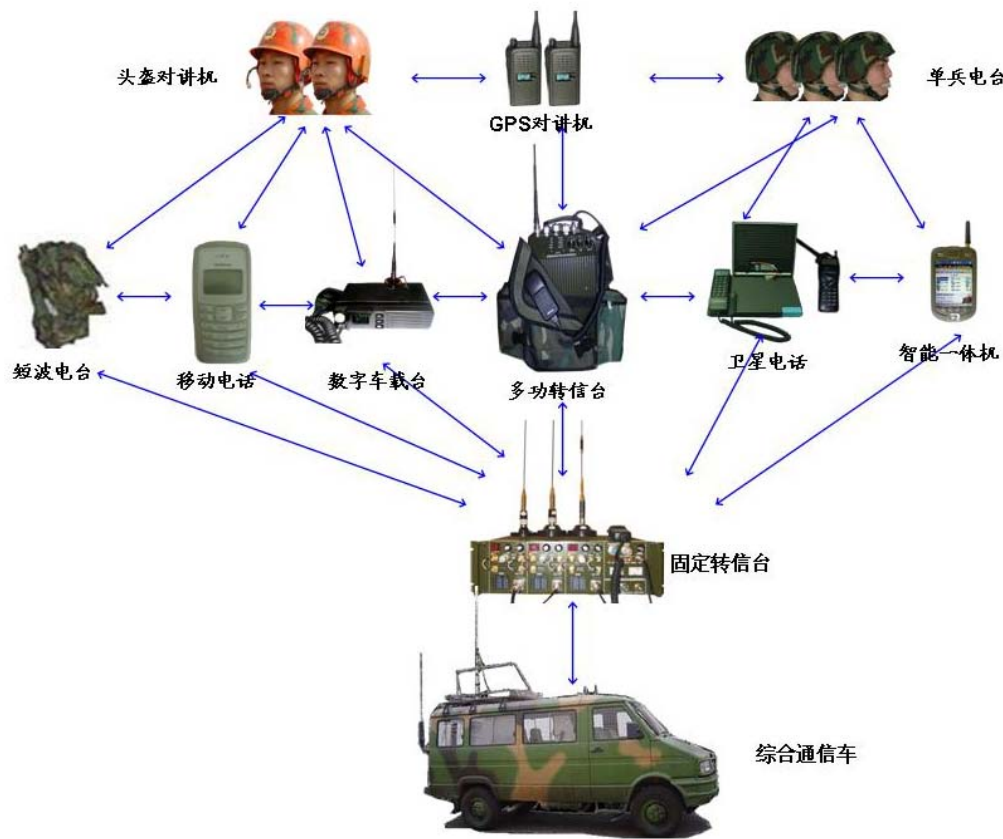


图 1 系统体系结构

班排对单兵通信：以近距离点对点话音通信为主，数据通信为辅，不需定位信息，能即时通信，具备单兵双手操作武器（具械）可进行通信及自组

织通信（不需要转信台支持）、有较强的抗干扰能力和一定的保密能力，是最基层的作战单元和最基本的作战行动。如图 2 所示。

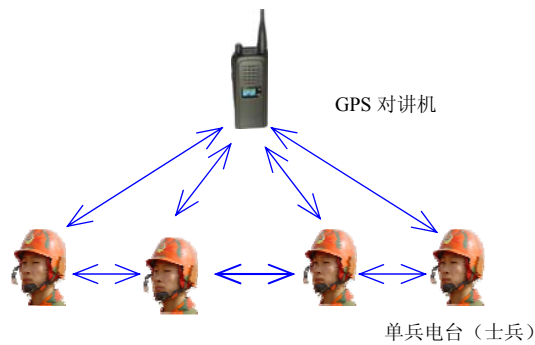


图 2 班排对单兵通信

大（中）队对班排通信特点是，除语音通信外，还具备 GPS 定位功能，军官电台可以对班排长电台进行准确定位，并能显示在 PDA 上，可扩展火灾现场通信距离，具备短信数据和文件互发的功

能，能与各种有无线装备进行互联互通，可与单兵电台和 GPS 对讲机构成二级指挥网。可保障机动的火场指挥调度。如图 3 所示。

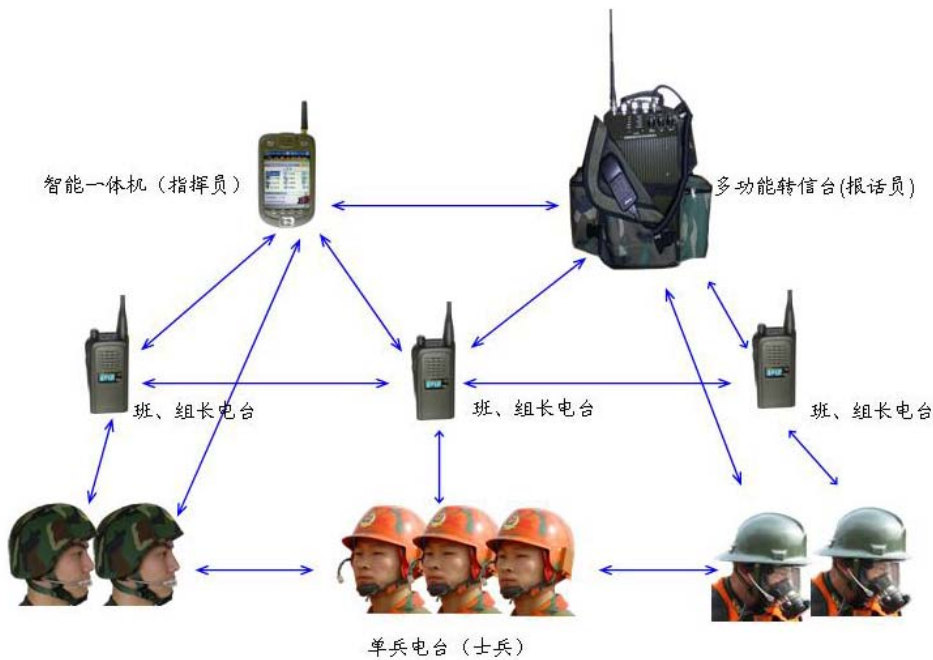


图 3 大（中）队对班排通信

前指对大（中）队特点是，前指指挥车具备 GPS 定位、超短波转信台、短波自适应电台、有线电话、传真，卫星电话等通信装备，在超短波车载电脑上可以安装地理信息（GIS）系统，可与 GPS

对讲机、大（中）队级通信网构成三级指挥通信网。能实时有效指挥控制部队，实现首长直接指挥到单兵。如图 4 所示。

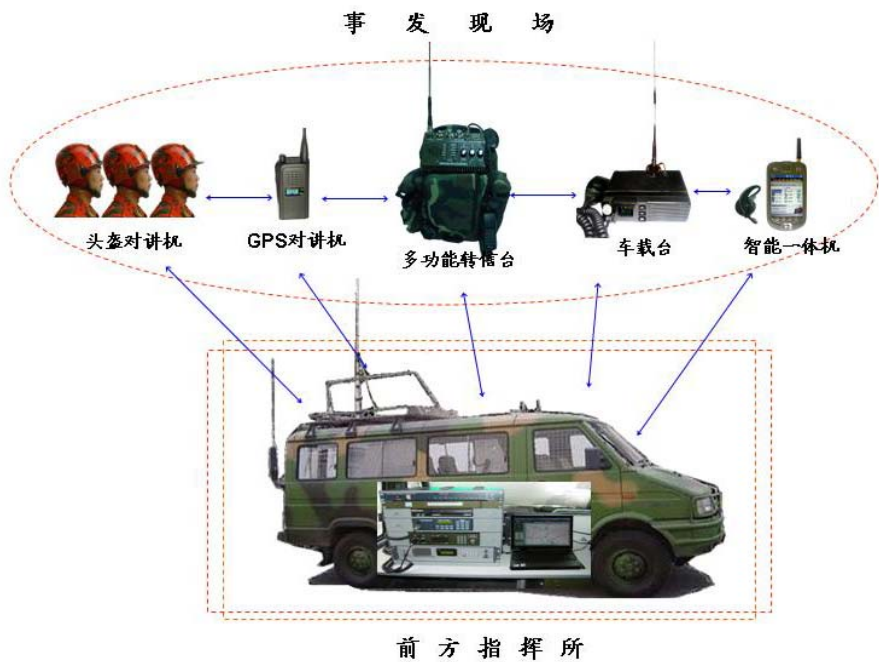


图 4 前指对大（中）队通信

基指对前指通信是指基本指挥所对方指挥所的指挥通信。其特点是基本指挥所（支队、总队、指挥部）可以通过固定电话网、移动电话网、超短波网、短波网和卫星网等有、无线通信手段接通前

指综合通信车进行互联，实现话音、图像等数据通信，并通过前指及时掌握了解火情信息、兵力部署和作战态势，以便做出正确的决策，及时下达作战命令。如图 5 所示。



图 5 基指对前指通信

武警森林部队战术机动综合信息系统是根据部队作战特点及通信建设现状，充分利用国内外民用通信技术创新成果的基础之上，构建的以超短波为基础，以智能控制软件技术为支撑，融无线通信、有线通信、卫星通信、计算机网络通信为一体，实

现语音、数据、图像综合应用的综合信息系统。它具有多平台软件协议融合及安全、边际智能功率控制、自组织通信、高速自纠错无线数传等多种优点，是解决武警森林部队通信指挥问题的重要手段。

参考文献（略）

作者联系方式

通信地址：北京紫竹院路 118 号武警森林指挥部通信处  
邮政编码：100097  
联系电话：010--88598716



# 强化信息管理能力运作促进军队作战能力提升

梁维泰

**摘要：**传统的指挥信息系统正向网络化方向发展，信息管理能力是网络化运作的最基本、最重要的能力，也是反映信息能力促进军队战斗力生成和提升的重要标志。本文主要就指挥信息系统在信息管理能力方面存在的问题，提出若干信息管理能力规则，并描述信息管理能力的运作过程。

**关键词：**指挥信息系统；信息管理；信息管理能力

## 1 引言

战斗力生成模式是战斗力生成的基本体系，是衡量军事系统效能状况的重要指标。信息管理能力是反映指挥信息系统运行效率的最基本、最重要的能力，进而也是反映着军队战斗力生成模式的最重要的标志。

信息化战争与机械化战争的战斗力内涵的本质区别在于信息能力的作用不同：机械化战争的信息能力只体现于对物质要素、精神要素和结构要素的保障与服务作用上；而信息化战争的信息能力不仅是战斗力新的组成要素，而且在战斗力诸要素中起着主导作用。信息时代的战斗力标准随之发生了变化，衡量军队战斗力的强弱更主要地要看其信息及管理能力的管理大小，制信息权将超越传统的制空权、制海权和陆地制权，伴随着制天权地位的凸显，成为军队主动权的主要标志。

战斗力和战斗力标准发生了本质变化，战斗力生成模式必然要随着战斗力和战斗力标准的发展而发展，其本质就是要从机械化战争依靠增强火力、机动力来提高部队战斗力生成模式向信息化战争依靠强化信息优势、决策优势来提高部队战斗力的生成模式转变。本文主要论述如何强化指挥机构的信息管理能力，以提高指挥信息系统获取信息优势、决策优势的能力。

## 2 存在问题

所谓信息管理能力是指为了支持决策而管理数据、信息和知识的能力。其主要内容是：通过有效的信息需求管理，数据、信息获取和处理管理，数

据、信息可访问性和可用性管理，以及由信息而生成知识的管理，达到有效支持作战决策和信息回馈的效果。

目前，传统的指挥信息系统正在向网络化方向发展，但有效的信息管理能力研究还未跟上。传统的信息管理程序过于复杂：在信息管理程序中，由于用户的作战行为中包含大量的信息交换，用户需要对接收到的信息进行层层过滤处理才能形成支持各种行动的作战图像，效率很低。这是由传统的信息“推送/下拉”方式造成的，不能有效解决巨量信息所存在的交叠、瓶颈、散播和超载现象，以至带来不利的影响。

1) 用户常收到远多于他们需要的信息。例如，一个基本作战单位不得不接收整个作战计划书，而分派给他们的任务只是其中的很小部分；

2) 这不仅给用户解析信息进而获取所需的信息造成麻烦，也给通信传输系统造成过载负担；

3) 需要为信息管理人员设置大量的人为接口来执行信息的解读，需要建立预期的信息收集、表述和分发来完成信息整合，最终才能生成作战图像。

当前，包括西方发达国家在内的指挥信息系统存在着如下影响信息管理的阻碍因素。

1) 虽然在获取信息优势能力方面取得了较大进步，但现行的环境中仍存在许多阻碍获取完全信息优势潜能的因素；

2) 战斗空间的感知信息频繁变化，并很快就会消失；

3) 对快速扩充的多源数据流进行整合（融合）的有效方法仍然很难找到；

4) 不能随时随地地应用近实时的方式对战争进行评估、计划和对作战进行指挥；

5) 需要评价当前使用的系统并确定它们能够提供什么的能力, 以及需要什么工具, 将哪些系统从一个多平台的松散集合转型为一个由网络紧密集成在一起的系统, 从而具备比各项能力总和更强的能力。

### 3 能力规则

如何解决作战指挥信息系统体系中存在的信息管理低效问题, 现提出如下信息管理能力规则。

(1) 将传统的“灌香肠”式的信息发布和索取方式改变为“灵活”的信息发布和索取方式

传统的信息“推送”样式反映了由于不恰当地“推送”信息所造成的困境。灵活的信息“推送”方式是假设由信息发送者来确定需要“推送”哪些信息, 传统的发送者只是将信息不加筛选的发布到网上, 灵活的“推送”者则只发布用户可能会感兴趣的信息。另一方面, 灵活的“下拉”则是一种面向需求的方法, 是由接受者决定哪些信息应当传输到网络。如果没有用户需求, 信息就不会被发布。

灵活的“推送”和灵活的“下拉”必须结合使用。灵活的“推送”提供的可能是用户尚未意识到需要的信息。这种方式是假设用户可能并不能了解其所有的信息需求或所有可获得的信息。缺点是发送者对信息需求的假设可能并不正确, 这将导致信息过剩, 造成网络负担。灵活的“下拉”允许用户规定网上信息的内容, 从表面上看, 这种方式似乎是更为有效, 但这取决于用户要了解其需求以及可能获得的信息。因此, “推送”和“下拉”两者要协调一致。如果经过培训的用户能够清楚明白地陈述其需求, 就能更为有效地“推送”信息。同样, 如果由知识丰富的信息“推送”者发布可获得的数据或信息, 就能更为有效地“下拉”信息。

无论是现在还是将来, 通信带宽都不是制约信息管理效率的关键因素。传统上, 解决方案通常都集中在通信信道的容量上。目前, 引起带宽超载更多的是由于信息管理低效而不是由于容量造成的, 本质上与低效的信息“推/拉”技术直接相关。缓解带宽问题的关键就是设计有效地信息“推/拉”规则。不仅要考虑发送什么信息, 还要考虑何时发送信息。1GB/秒的下载有可能会造成网络负担, 但如果发生在适当的时间, 并不会降低网络能力。这

与水坝的情况类似, 要规范水坝的泄水以确保在缓解水坝的蓄水压力的同时又不造成水灾。灵活的“推送/下拉”技术将可以提高网络中心环境下的信息管理效率。

#### (2) 优先考虑决策质量信息

所谓决策质量信息是信息管理过程为指挥主官提供“恰当”的输入信息, 由此获得“正确”的决策选择。作战指挥机构要良好地运行, 指挥主官必须做出正确的决策。虽然拥有完善的信息并不能保证做出正确的抉择, 但利用高质量信息, 决策者可以管理地更好。通常情况下, 指挥主官被授权做出关键的决策, 而大部分决策将决定其机构的运作功效。未来信息管理过程将为指挥主官提供“恰当”的输入从而做出“正确”的选择。而“恰当”的输入就是所谓的决策质量信息。当高层指挥主官做出的关键决策输入到下一机构, 机构的最优先任务就是识别这些决策, 从而确定支持这些决策的信息需求。

并非所有的信息都是决策质量信息, 也并非所有的信息都是无用信息。在一个机构中有可能需要非决策质量信息, 过程和系统要支持此类信息的生成, 但要避免无用或多余的数据/信息。未来信息处理过程将选择“恰当”的信息, 特别是那些对决策者有用的信息。那种认为信息管理过程将使通信过程变得完美无缺的想法是不切实际的, 但通过把重点放在决策质量信息和所支持的决策上, 信息管理过程将从根本上改进通信过程。

#### (3) 选择或分解信息

灵活的“推送/下拉”能够缓解带宽过载, 而通过选择或分解信息也可缓解带宽过载。所谓选择或分解信息, 就是按用户类型向用户发送不同类型的信息。如, 电视观众对所看的新闻信息没有选择能力; 报纸读者则有少许的新闻选择能力; 而互联网则为用户提供了更有选择性的新闻信息。通过信息选择或分解, 将能够以高效率提供信息产品。作战计划的大小与分配任务的数量有关, 但多年来, 作战计划可能都以完整下达到所有相关部队, 各受命部队不得不在整个计划中找寻并处理仅对自己有用的很小部分的信息。今后, 通过信息选择和订阅应用, 各机构可接收和选择处理所需的任务分配信息。

#### (4) 利用信息资源刻画正确的图像

也许今后若干年, 信息管理能力还不能适应自由输入的信息流, 但可通过定义公共信息集合, 即



提供了一个按等级分组的信息集合来有效管理信息。

所定义信息集合的底层是原始信息资源,由用户所需的基本信息构成的实体,如起飞时间、目标数据、雷达回波和图像等;第二层定义为信息交换产品,是信息资源以及支持活动所需的其他输入的集合,其表现形式是传感器的输出、情报、文电、计划、指令等。最上层定义为公共相关作战图像,是由相关信息交换产品融合形成的满足不同类型用户相同需求的信息集合,其表现形式是战场态势、装备状态等。

不同级别的机构有不同级别和类型的公共相关作战图像,他们中的信息资源可以共享;高层机构的公共相关作战图像可由所属机构的公共相关作战图像融合而成,而低层机构的公共相关作战图像可以由高层机构的公共相关作战图像经过裁剪而形成。

#### (5) 开发利用可获取共享信息空间

可获取共享信息空间是描述所建立的根据特定作战需要而划分的共享空间,可分别以任务、功能和威胁等为中心。根据任务,如空中支援、封锁等,或跨任务、机构或联合部队的作战威胁建立一个可获取共享信息空间。如,时间敏感目标就是一种有多个作战实体参与的可获取共享信息空间。可设置专门的机构负责分配可获取共享信息空间并授权用户访问,但信息的拥有权归信息的所属机构,各成员在可获取共享信息空间中进行协作。

#### (6) 建立协作共同体

协作共同体是指为寻求共同目标、利益、使命或业务程序必须交换信息的协作用户团体或者因此必须对交换信息具有共同定义的机构,通常既包括信息生成方也包括信息使用方。协作共同体按作战需要有不同的划分方式,可按照机构职能来划分(如统帅部空军、海军、陆军部位),也可按地理或地区划分(战区方向空、海、二炮联合打击部队)。位于高层的协作共同体代表的是公共指挥实体和指挥系统,是为支持整个所属机构的协作服务,而不仅仅为该机构服务。协作共同体的构造可以有效地管理和应用共享信息。

#### (7) 建立信息管理组织

高效的指挥机构运作需要信息管理能力来支持。建议师/团级以上机构可设立三层级别的信息管理组织:信息管理官、信息管理处和信息管理

员。

信息管理官掌管指挥机构的所有信息管理活动,负责与外部信息管理官和机构进行协调,负责发布信息管理计划。信息管理官应密切关注最高指挥主官的信息管理需求,拥有授权协调行动和过程以满足基本的信息需要,与上级信息管理官紧密合作,确保所需的信息上传。

信息管理处在信息管理官的领导下工作,在指挥机构主官的监督下运作。信息管理处的成员来自机构各职能部门,以解决机构内部的、跨职能的、以及在上级指挥机构信息管理部门指导下的信息管理问题。

信息管理员是信息管理处的成员,也是指挥机构信息管理具体执行者,主要协调机构内的信息管理活动。信息管理员要确保机构的信息管理策略和程序在责任区内得以实施和遵守,负责为信息的全生命周期管理提供过程与业务准则,并为通用软件应用程序提供帮助。

上述七条规则确定了指挥机构信息管理能力的运作模式。通过建立信息管理组织,直接与指挥机构、信息生产者和消费者、内部和外部的网络,以及与网络相关联的各种系统进行互动合作。信息管理能力主要体现在使分类用户通过产生信息请求有效的获取信息,包括通过构造可获取共享信息空间和划分协作共同体,利用信息资源、信息交换产品和通用相关作战图像来刻画指挥机构的信息过程等。

## 4 运作过程

根据上述信息管理能力规则,结合网络化的指挥信息系统的实际需求,描述信息管理能力的运作过程。

### (1) 建立信息管理能力

第一,需要统帅部信息管理官与战区级和部队的联合部队指挥机构信息管理官共同建立网络中心的信息控制过程,以用于推动和支持信息管理任务的执行。网络中心的信息控制过程还要监督网络中心的基础设施开发利用。信息管理能力按照确定的规则来控制机构内的信息管理程序。

第二,建立各级指挥机构完善的信息管理组织,包括信息管理官、信息管理处以及信息管理员。信息管理官的职责包括:指导机构信息管理计

划的制定、了解和掌握作战节奏、监督机构指挥主官信息需求的管理、监督信息请求的管理、领导信息管理处的工作等；信息管理处的职责包括：与其他机构的信息管理处互动合作、协调机构指挥主官信息需求、管理初始的共享信息空间分配、管理信息请求等；信息管理责任包括：具体的信息资源和设施管理、提供全面的信息管理技术支持、管理电子文件、管理消息服务等。

第三，建立指挥机构指挥主官信息需求，是由机构指挥主官确定的信息需求经优先级排序后形成的清单，对于理解作战流程、辨别风险、及时制定决策是至关重要的。信息需求包括，作战环境类、友军类、威胁类等。

第四，建立信息管理战略与计划，是描述机构管理网络中心信息计划的方法，以及方法是如何支持外部机构和上级信息管理计划的。包括：描述信息管理组织、提供指挥主官的信息分发策略、描述信息需求、说明协议准则和作战计划连续性等。

第五，建立并实时更新机构的数据标准、指标和用户类型。

## （2）管理信息的可访问性

第一，提供信息存取服务，即为用户提供可用服务清单，以及说明所有可预定的机构信息资产清单。

第二，处理机构信息需求，用户可要求当前处于某清单目录中的网络中心信息资产的访问权，或对某个已分类的信息资产的修改，或建立新的（未分类的）信息资产，或预定网络中心信息产品，如公共相关作战图像等。

第三，管理共享信息空间，各级信息管理官根据作战需求，为所属机构分配共享空间，并为机构相关的任务、功能、威胁等建立更细的共享信息空间。信息管理官分配机构的共享空间并且对必要的机构授予访问权，所有信息资产和信息交换产品可

在单独的或协作的环境中使用。

## （3）管理组织的信息处理

第一，定义机构的实体，主要是建立能反映机构对共享信息理解的机制。包括信息分类方案、类属词典、词汇表、关键词列表和分类法。主要开发：机构的信息方案定义、维护机构的类属词典和关键词列表、机构的分类法定义和维护机构的词汇表等。

第二，确定信息资产需求，包括关于资源、概要内容、安全和格式描述符的信息。

第三，将元数据与信息资产结合，即为所有要存储到共享信息空间的信息提供发现元数据包括，应用安全描述符、应用资源描述符、应用概要内容描述符、应用格式描述符和应用可扩展层等。

第四，将信息资产存储到共享信息空间，使机构共享信息空间中的信息可用。共享信息空间提供存储和服务机制，存储到共享空间的机构信息通过相关的元数搜索方法发现。

## （4）管理网络中心的图像和产品

标准的、网络中心的公共相关作战图像，是各级指挥机构的最终信息产品，它建立和维护至关重要。

首先，处理机构公共相关作战图像的生成请求，按照作战需求、共享信息空间需求和互联需要来分析，确定公共相关作战图像的生成需求。

第二，生成机构的公共相关作战图像，通过信息预定，格式化、共享信息空间访问权和需求的确认，生成公共相关作战图像。图像经信息管理官批准，可以发布和操作。

第三，发布并监控机构的公共相关作战图像，信息管理处发布新的公共相关作战图像到授权用户，同时监控公共相关作战图像的运行情况，生成状态报告。

## 参考文献（略）

## 作者联系方式

通信地址：C<sup>4</sup>ISR 技术国防科技重点实验室（28 所分实验室）

邮政编码：210007

联系电话：025—84288021

# 一种基于平流层通信的分层立体化网络组网方式

黄建洋 张洪永 王靖

**摘 要:** 本文以平流层通信为基础, 构建了以平流层飞艇、无人机、地面终端等节点组成的空地一体的分层立体化网络, 给出了这种分层立体化网络的分布式组网方式及其网络模型, 并阐述了这种组网方式的主要优势及其关键技术。

**关键词:** 平流层通信; 组网方式; Ad Hoc

## 1 引言

平流层通信是指在距地面 20 km 至 50 km 的平流层使用稳定的通信平台作为中继或交换中心, 与地面控制设备、入口设备以及多种无线用户构成的通信系统, 可以提供多用户、多用途的各种固定、移动通信业务<sup>[1]</sup>。平流层通信因其具有良好的电波传播特性、通信容量大、组网灵活等优势而受到世界各国的普遍重视。

利用平流层飞艇具有特定高度、长驻空, 准静止、可承载一定规模有效载荷的特点, 通过其提供的空中骨干信息管理设备, 将其与无人机、空飘气球、地面终端等信息节点进行空空、空地互联组网, 改变了传统通信网络主要依靠地面节点组成平面型网络的方式, 形成了空地一体的分层立体化网络, 大大扩展了通信范围, 提高了移动用户的持续移动通信能力, 使之在地理测绘、信息传输、数据广播、导航定位等方面具有无可比拟的优势。

对于这样全新的空地一体化网络, 采用自组织、分布式的 Ad Hoc 组网方式, 无疑能更好的发挥网络自身的特点, 通过对其网络特性的研究, 能够有效提升网络的整体性能。然而, 在如此大规模网络中(节点数目成千上万), 采用 Ad Hoc 这种分布式自组织网方式必将是一个严峻的挑战。由于网络拓扑高速动态的变化和大量节点不可预知的移动性, 给网络管理、路由选择、QoS 设计带来了极大的困难。本文给出了这种基于平流层通信的分层立体化网络的分布式组网方式, 并阐述了这种组网方式的主要优点及其关键技术。

## 2 基于平流层通信的分层立体化网络的组网方式及其优势

传统的基于平流层通信系统的设计思想主要是在平流层这一高度(20~40 公里)布置平流层高空通信平台作为通信的中继站或交互中心, 与地面控制设备、入口设备以及多种无线用户相联接而构成一个覆盖式的通信系统。我们在加入无人机、空飘气球等空中信息节点后, 采用分布式的自组织网方式, 剔除了平流层高空平台绝对中心的概念, 使得整个系统在网络覆盖、信息处理等方面得到大大的加强, 但同时也大大提高了网络的复杂度。针对网络的基本结构, 我们采取分层立体化的设计思想。同时考虑到无人机、空飘气球在空中的地理位置(8~10 公里), 以高度来划分, 提出了三层结构的组网方式。

### 2.1 组网方式

在整个分层立体化网络中, 大量地面终端节点(用户终端、网关、系统控制站等)组成地面网络, 构建第一层子网, 空飘气球、无人机等节点组成第二层子网, 平流层飞艇节点组成第三层子网。整个网络结构是自形成、自组织、自修复的。所有节点均能够快速加入、离开和重新组织, 全网能够做到信息互通, 节点通信时均能实现最短跳数通信。图 1 给出了基于平流层通信的分层立体化 Ad Hoc 网络模型。

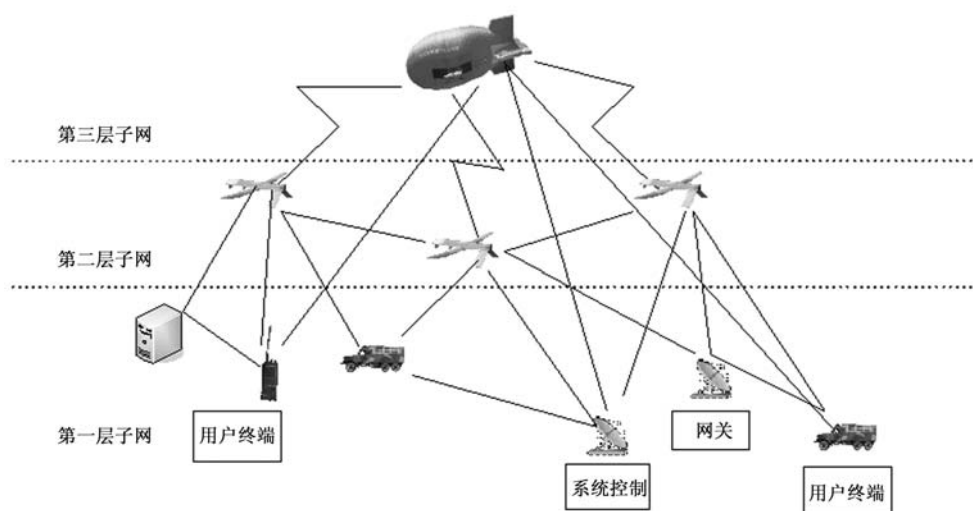


图1 基于平流层通信的分层立体化 Ad Hoc 网络模型

在这样一个分布式自组织 Ad Hoc 网络中，从第一层子网到第三层子网，节点数目依次递减，其网络节点的容量、覆盖范围、处理能力呈上升趋势，层与层之间、节点与节点之间的信息可以完全共享，这大大扩展了通信范围和通信能力。完全分布式的自组织网方式改变了传统的以平流层飞艇为中心的单一组织模式，既充分利用了平流层飞艇平台自身通信容量大、处理信息能力强的优势，又大大提高了整个网络的抗毁、抗干扰能力，使得整个系统的性能得到跨越式的提升。

在基于平流层通信的分层立体化 Ad Hoc 网络中，由于平流层飞艇通信链路宽、容量大，整个网络支持的业务方式将非常灵活，既适用于人口密集的城市，又适用于人烟稀少的野外；既适用于固定宽带接入业务，又适用于移动业务；既适用于窄带通信，又适用于宽带通信。

## 2.2 组网优势

基于平流层通信的分层立体化网络其分布式组网模式有许多明显优势，通过对整个网络特性的研究可以弥补发达地区与欠发达地区在通信领域的差距。其突出优势可以概括为以下几个方面。

1) 在基于平流层通信系统构建的分层立体化 Ad Hoc 网络中，平流层通信信道衰落小，具有良好的电波传播特性。同时，与卫星通信系统相比，平流层信息平台与地面的距离只有卫星高度的 1/1800（高轨）、1/400（中轨）、1/40（低轨），无

线信号传播延迟小（从 250ms 减少到 0.5ms）、自由空间衰减分别减少 65dB、52dB 和 32dB<sup>[2]</sup>，有利于通信终端的小型化、宽带化和毫米波化。

2) 在基于平流层通信系统构建的分层立体化 Ad Hoc 网络中，利用第三层子网节点（平流层飞艇）部署灵活，覆盖范围大的特性，使得下层通信节点可以利用上层节点的超视距一跳中继能力，显著降低信息的路由转发次数，大大减少了高层建筑、山坡及其他妨碍通信的障碍物所引起的电波传播遮挡现象，一定程度上减少了多径传播的影响。这一设计，使得传统的、复杂的地面通信系统的网络结构大大简化，而网络容量及传输容量则成倍增加。

3) 平流层通信系统造价低廉，相比通信卫星，价格仅其一半，而且无需发射费用。虽然覆盖范围比卫星小，但可以满足国土内重点区域通信覆盖的要求。平流层信息平台可以回收，维护简单方便，技术风险比较低。平台的回收不会产生空间垃圾，有利于环保和可持续发展。整个系统面向综合业务接入设计，系统的效费比高。

4) 基于平流层通信系统构建的分层立体化 Ad Hoc 网络，全网分布式运行，信息获取和利用手段多元化、一体化，节点补充替换容易，机动性能好，抗毁能力强，在军事通信中有很好的发展前景。

### 3 基于平流层通信的分层立体化网络的关键技术

针对基于平流层通信的分层立体化网络,有许多关键技术值得进一步研究。

#### (1) 方向性天线技术

传统的全向天线的 Ad Hoc 网络面临着网络容量受限、传输能力受限、信号易被干扰等重要问题,要有效地解决这些问题,方向性天线具有独特的优势。方向性天线由于其窄波束特性,能带来乘性的空间复用度增加,提高网络容量;能在不增加发射功率的情况下有效增强设备的传输能力;能有效提高信号抗截获能力和抗干扰能力。要充分发挥方向性天线的优势,一要加强方向性天线关键算法研究,重点研究适合高动态拓扑、恶劣电磁环境下的自适应算法;二是要联合 MAC 层和物理层实现自适应功率控制的跨层设计,重点解决由于方向性天线的使用导致自组网出现“听不见”和新的隐终端问题。

#### (2) 路由选择技术

新的组网方式使得对路由算法的设计要求更高。传统的平面结构的路由算法显然不适合分层结构的大规模立体化网络<sup>[3][4]</sup>:随着网络节点数的增加,路由受网络拓扑变化的影响越明显,单一节点的吞吐量迅速下降直至零;当网络规模较大时,路由协议的控制报文开销将会占据很大一部分可用带宽,从而导致网络性能的急剧下降。而层次结构的 Ad hoc 网络路由其复杂的簇头选举算法、簇头为网络的瓶颈、受限于无线传输的衰落和干扰特性,使得路由协议的移动管理较为复杂,路由协议的性能难以得到突破性的提升。因此在方向性天线窄波束、网络节点移动速度快的双重特性下,要加强对路由选择和路由维护的研究,重点是研究快速的路由重定向问题,并建立完善的仿真实验系统进行建

模分析,从而为实际的网络建设提供技术支持。

#### (3) 通信频段的选择

WRC-1997(世界无线电大会)确定将 47.2~47.5 GHz(下行)和 47.9~48.2 GHz(上行)共 600 MHz 的频段在世界范围内分配给平流层通信平台使用。考虑到雨水对毫米波吸收的影响,WRC-2000 建议研究使用 18~32 GHz 范围内的频段,特别是考虑使用 27.5~28.35GHz、31.0~31.3GHz 频段<sup>[5]</sup>。由于这个频段已经在卫星通信系统中取得了成功,没有给平流层通信系统预留使用频率,通常的做法是采用频率反转的方式,即以卫星通信系统的上行频段作为平流层通信系统的下行频段,以卫星通信系统的下行频段作为平流层通信系统的上行频段。在这种方式中,关键是如何避免或减少系统间的相互干扰。当前另一种方案是采用频率为 2GHz 左右的频段。2GHz 频段的电波能够穿透建筑物或其他障碍物而在移动终端间建立通信链路,已在地面和移动通信系统中取得了巨大成功。ITU 一直致力于解决如何使用和分配 2GHz 的频段问题,以增强系统的互通性和兼容性。加上基于平流层通信的分层立体化 Ad Hoc 网络包含各种不同用途的电子设备,其内外部的电磁环境都比较复杂,电磁兼容性也是必须要考虑的突出问题。

## 4 结束语

利用平流层通信平台构建分层立体化 Ad Hoc 网络,理论上能够进一步深入探索空间立体组网、异构网络互联与复杂网络传输等复杂课题,实际应用中能够在国防建设、数字通信、气象预报、自然灾害监控等众多领域发挥重要作用,其研发工作的进展对我国的科技创新、国防建设和国民经济发展具有十分重要的战略意义。

#### 参考文献(略)

#### 作者联系方式

通信地址:北京市丰台区大成路 13 号 T01

邮政编码:100039

联系电话:010-66820244 15901515216

# 军事通信网络管理系统

莫世禹 李冷冷

摘 要：本文介绍军事通信网络管理系统的需求、主要功能、体系结构及设计原则等内容。

关键词：军事通信网；网络体系结构；网络管理

## 1 需求分析

未来高技术战争，其战场将是海、陆、空、天、电五维战场于一体的信息化战场，是全空域、大纵深的立体化、突发性、快节奏的高技术战场。目前，各国军方正正在加紧研究有关信息战的基本特征、实施原则、战技、战法以及它对将来的战略战术和武器系统的影响等等，其目的在于争取未来信息战的主动权。通信作为信息传递的主要方法和手段，是获得全时空的制信息权的基础措施。通信业务和网络技术正在迅速发展，业务提供者的竞争日益激烈，用户对新业务的需求，也在与日俱增要适应这种趋势的变化，必须建立自动化、集中化和智能化的网络管理系统（NMS）进行支撑。

### 1.1 建设军事综合通信网络及其管理系统是未来信息化战争的需要

传统通信网络存在以下很大的局限性

1) 没有统一的体系结构规划，系统之间基本上是相互分离的相互各自独立的烟囱式系统。

2) 封闭的专用系统缺乏联网标准，其联网协议不是开放的，也不是分层的，难以实现互联互通和一体化无缝复盖。

3) 缺乏灵活性，智能化、自动化水平低，系统部署之前需要做大量的频率分配，密钥分发，指定网络名称和主机地址等预先规划工作。

4) 以传送话音业务为主，无良好的“数据运载体”，难以适应战术数据，通用作战图象和目标指示信息的传输。

5) 没有相关的信息网络规划，缺少统一的系统管理，整个系统网络运行效率不高，通信质量难以保证。

6) 没有网络安全的总体计划，缺少信息安全

保证体系的顶层设计，影响信息的共享。

7) 缺少抗侦察、抗干扰、抗摧毁、抗入侵的有效技术措施，不能适应现代电子战和信息战对抗的需要。

### 1.2 建设军事通信网络管理系统有利于采用统一的体系结构规划

建设军事通信网络管理系统有利于采用统一的体系结构规划，整合现有各系统资源，把相互分离相互各自独立的烟囱式系统变成扁平式系统，实现综合系统集成，形成协同作战（CEC）能力。

### 1.3 建设军事通信管理系统有利于采用统一的标准

建设军事通信管理系统有利于采用统一的联网标准，开放的、分层的联网协议，易于实现对异构网管理，特别是对老式网络的管理，易于实现互联互通和一体化无缝复盖；有利于根据编队网络的移动特点实现主机和网络（节点）的移动管理。

### 1.4 建设军事通信网络管理系统有利于实现通信网络的扩容

新业务的不断出现及新业务的使用方便，大大地刺激了用户的需求，用户接入网的概念应运而生，特别是按需分配带宽和按需分配业务以及不失实效的优良服务给用户带来极大的满足。与此同时，新业务对传统的管理模式带来巨大的冲击，指挥管理方式都必须做出相应的变革。这种冲击和变革需要有相应的组织机构适应，这就是现代化的网管系统。为使新业务使用方便、高效并迅速推广，相应的要尽量减少网络运行的成本，或者说要有效地充分利用网络资源，并使新技术、新业务尽快转化为生产力和战斗力。网络资源充分利用的程度取

决于网管系统的先进程度。目前,提供通信设备制造的厂商其硬件设备的技术水平和性能指标都相差无几,其差别主要体现在设备对网络管理支持的先进程度上。各通信装备制造厂商争相与计算机公司联合共同开发网管系统。今后的通信设备都具有网管配套装置,如没有先进的网管系统与之配套,再先进的装备也难以发挥出全部效能。

### 1.5 建设军事通信网络管理系统有利于实现向C4ISR及GIG过渡

军事通信网络管理系统的建设必然是在全军的信息化建设的大环境下进行的、是在全军顶层设计的框架上进行的,是全军信息化建设的需要,因此易于实现向 C4ISR 及 GIG 过渡。

## 2 国内外发展状况

在国内,军事通信网络管理系统发展比较迅速,但三军尚未形成完整的、统一的体系,有待进一步发展。

在国外,已经运用了当今世界上最先进的通信技术,美军海军提出了网络中心战的概念,美军完成了全球指挥、控制、通信、计算机、情报、监视及侦察系统(C4ISR)的构建,并在构建全球信息栅格(GIG);实现了战争从以平台为中心到以网络为中心的根本性转变。网络中心战快速、安全可靠地用网络把不同的、地理上分散的作战人员和平台连接在一起,进行资源和信息的共享,从而达到部队战斗力的最大化。

## 3 军事通信网络管理系统的主要功能

通信网络管理功能是通信网络管理系统的关键部分。早在 1984 年国际电联对电话网管理就作了如下的定义:“监视网络运行,在必要时,采取行动控制通信流量的功能。”网络管理的要求是对运行中的网络状态和性能进行实时监控和测量,并具有立即控制业务流量流向的能力,达到尽可能高的呼叫接通率,使网络设备和设施发挥出最大的效益。国际电联的网管功能总称为 OAM&P,即运行、管理、维护和指配。Operation 运行功能是指支持网络业务的管理;Administration 管理功能是

检验网络服务水平和网络资源使用的最佳化;Maintenance 维护功能是负责改正和预防故障的管理;Provisioning 指配功能是支持提供服务的网络配置。基本的 OAM 原则是以网络控制和维护为基础的。

### 3.1 军事通信网络管理系统的管理功能

- 1) 确定管理参数
- 2) 网络管理参数的管理
- 3) 获取网络运行状态
- 4) 分析网络运行状态
- 5) 实施对网络的控制

### 3.2 军事信网络管理系统的性能管理

- 1) 性能管理参数
- 2) 性能指标管理
- 3) 性能监视
- 4) 性能分析
- 5) 性能控制

### 3.3 军事通信网络管理系统的故障管理

- 1) 维护策略
- 2) 故障管理参数
- 3) 故障指标管理
- 4) 故障监视
- 5) 故障定位和测试
- 6) 故障恢复

### 3.4 军事通信网络管理系统的配置管理

- 1) 配置管理参数
- 2) 网络规划
- 3) 网络指配与配置控制
- 4) 配置监视

### 3.5 军事通信网络管理系统的账务管理

- 1) 账务管理有关的管理参数
- 2) 费率管理
- 3) 计费、摊账和审计

3.6 军事通信网络管理系统的安全管理

安全管理就是控制进网和保护网络及网管系统，防止有意和无意的滥用，未经许可的接入和通信的丢失。安全管理有两层含义：一层含义是对管理对象——通信网——进行安全管理，保证通信网的安全；一层含义是对网管系统本身的安全管理。

- 1) 风险分析功能
- 2) 安全服务功能
- 3) 告警、日志和报告功能
- 4) 网络管理系统的保护功能
- 5) 常用的安全机制

通信网络管理系统中常用的安全机制有：身份鉴别和接入控制

3.7 军事通信网络管理系统的拓扑管理

- 1) 拓扑信息获取

专业网络管理系统要根据网络配置信息自动或人工生成拓扑结构，存入拓扑数据库

- 2) 拓扑信息指配
- 3) 网络拓扑结构的显示
- 4) 拓扑信息过滤
- 5) 拓扑图操作

3.8 军事信网络管理系统的系统管理

- 1) 系统访问日志管理
- 2) 系统操作日志管理
- 3) 系统登录和操作控制
- 4) 系统支持

系统支持包括帮助子系统、网管系统软件模块运行状态的监视与控制、网管系统硬件设备运行状态的监视等管理功能。

3.9 军事通信网络管理系统的用户管理

- 1) 增加用户
- 2) 删除用户
- 3) 查询用户属性
- 4) 修改用户属性

3.10 军事通信网络管理系统的资源管理

资源管理主要指对与网络有关的设备、设施以及网络操作、维护和管理人员进行登记、维护和查阅等一系列管理工作，通常以设备记录和人员登记表的形式对网络物理资源和员工实施管理。设备记录中要记录网络中使用的每个设备的参数设置、设备利用率统计结果、有关制造厂家的数据、备用零部件数量及其储存地等信息。

4 军事通信网络管理系统的功能体系结构

军事通信网网络管理系统由管理信息传输系统、专业网络管理系统、综合网络管理系统、通信指挥管理系统、安全保密系统五部分组成。其中，管理信息传输系统是基础，专业网络管理系统是系统的基本组成部分，综合网络管理系统是系统的核心，通信指挥管理系统是系统提供的智能化的通信指挥手段，安全保密系统是系统安全可靠运行的保障。军事通信网网络管理系统功能体系结构如图 1 所示。



图 1 军事通信网网络管理系统功能体系结构



## 5 军事通信网络管理系统的技术体系结构

军事通信网综合管理系统主体构架采用国际电联（ITU—T）建议的电信管理网（TMN）技术体制。

系统网络管理协议：包括通用管理信息协议（CMIP），简单网络管理协议（SNMP），公共对象请求代理体系结构（CORBA），以及各系统设备厂家专用协议。

系统管理功能：TMN 通常包括性能管理、故障管理、配置管理、计费管理、安全管理五大管理功能。但在军事通信网综合管理系统中，结合军事通信网管理实际以及通信指挥的需要，系统管理功能还应包括系统管理、拓扑管理、任务管理、资源管理、用户管理等管理功能。

管理层次结构：包括事务管理层、业务管理层、网络管理层、网元管理层。

## 6 军事通信网络管理系统的设计原则

军事通信网网络管理系统的设计原则应与军事通信网当前实际和发展的目标相适应，既要满足实际需求，又要符合未来发展的需要。具体内容如下。

### （1）实用化

系统应满足军事通信网网络管理的实际需要，有利于提高通信网的自动化和科学化管理水平，有利于通信保障能力的提高。同时，系统的设计和实现应具有先进性，使系统具有可持续发展能力。

### （2）自动化

通过自动化的技术手段，实现通信网络监测、

控制、调整、故障定位和维护管理自动化。

### （3）综合化

在统一的管理平台上，对军事通信网实现集中统一的综合管理，实现不同专业网系间的网络配置和运行信息共享，实现多个专业网络管理系统之间的互连、互通、互操作。

### （4）智能化

系统要具有智能化的故障发现与恢复功能以及辅助决策功能。

### （5）标准化

采用先进成熟和通用的技术标准，实现系统平台、信息模型以及接口协议的标准化，使系统具有良好的开放性和接入能力。

### （6）模块化

系统软件设计应采用软件工程方法和模块结构，系统功能模块应能灵活配置。

## 7 结束语

军事通信网络及其管理系统的研制及建设是一项复杂的系统工程，它涉及的面很宽，技术非常复杂，几乎集中了现代 IT 产业的所有高新技术，其地位极为重要。军事通信网络管理系统设计的建设应以新时期军事战略方针为指导，以提高军事通信网的综合保障能力为宗旨，遵照“统一体制、统一标准、逐步演进、总体规划、分步实施、技术先进、自主开发”的原则，遵循国际电联（ITU—T）提出的电信管理网（TMN）的框架和规范，建立与国家公用网管理技术体制相一致，具有我军特色的通信网网络管理体制，形成综合、高效、实用、可靠、灵活、安全，便于发展的军事通信网网络管理系统。

### 参考文献

- [1] 王厚生, 郭淦水. 军事通信网网络管理. 北京: 军事科学出版社, 2002 年 2 月第 1 版
- [2] 扬义先, 钮心忻, 李名选. 网络信息安全与保密. 北京: 北京邮电大学出版社, 2001 年 11 月第 2 版
- [3] 舒治安. 适应信息化战争的军事通信网络发展研究, 中船重工集团第七二二研究所, 2005 年报告

### 作者联系方式

通信地址: 武汉市 70005 信箱

邮政编码: 430079

联系电话: 027-87927773/13607186049

# 装备维修保障信息的集成化IETM系统技术研究

安钊 徐宗昌 郭红芬

**摘 要:** 根据装备维修保障信息集成化的趋势, 本文提出以交互式电子技术手册为基础, 集成各种信息管理系统, 提出了一种集成化 IETM 系统的框架, 将维修技术文件和维修过程的业务处理紧密结合, 并分析了集成化 IETM 系统关键性技术。为装备维修保障信息的信息集成提供了一种思路。

**关键词:** 技术保障信息; 集成化; IETM 系统

技术文件是实施维修保障的基础和依据, 是装备维修保障信息的载体。传统的设计思想将修理文件查询系统和日常业务处理系统隔离开来, 分别设计和各自独立运行, 这必将给我们的修理工作带来极大不便, 无法实现装备维修保障的一体化管理。因此, 将技术文件数字化, 实现装备修理技术资料与业务管理系统的集成, 在同一个数据库层面综合装备修理过程的计划进度、器材库存、故障分析、修理质量评估和人员培训等方面的数据, 是提高我军装备保障整体信息化水平的一种需求。

## 1 技术文件数字化

修理人员主要依靠纸介质的技术手册来查询装备的修理工艺、零件鉴定标准和质量检验标准。使用的纸介质技术手册, 不仅重量与体积大、而且查询不便, 当装备改装时, 技术手册内容的更新困难, 无法找到相应数据, 降低了保障分队的保障能力和装备的战备完好性。随着武器装备复杂程度的提高, 设计、生产、使用和修理过程中的技术数据已成为一个庞大的系统, 若将这些数据变成纸质技术手册时, 利用它来查找各类维修技术手册的时间是难以想象的<sup>[1]</sup>。可见, 技术文件数字化是必然要进行的。

交互式电子技术手册 (Interactive Electronic Technical Manual, IETM) 是由装备的制造者或使用者采用自动编辑系统创作的, 以数字形式显示在屏幕上, 能为终端用户提供技术信息的电子显示系统, 其本质是一种技术手册<sup>[2]</sup>。IETM 出现于 20 世纪 90 年代, 目前已成为美国等许多发达国家所推行的 CALS (持续采办与寿命周期保障或光速商务) 战略的重要组成部分, 也是装备保障信息化技

术研究和应用的热点之一。

## 2 集成化IETM系统的设计

### 2.1 集成化IETM系统总体结构

根据功能需求及技术实现手段, 设计了维修保障中的集成化 IETM 系统。集成化 IETM 系统由综合数据库、阅读器及管理系统三部分组成。其总体结构如图 1 所示。

综合数据库包括业务数据库和 IETM 库, 业务数据库记录修理过程中的各种业务数据, IETM 库存储各种技术资料, 底层由技术信息库和课件库构成。阅读器用于交互式查询, 能够同时获取业务数据和 IETM 库的信息。管理系统包括业务管理系统、技术信息管理系统及课件管理系统, 业务管理系统完成业务过程中的计划拟制、作业调度、器材管理等功能, 技术信息管理系统完成技术数据的录入、录出、修改等功能, 课件管理系统实现图形素材与培训所需的音频、视频及动画素材管理, 中间件 (逻辑引擎) 完成当前任务所需的技术信息与相关课件、素材的链接。数据交换标准采用 XML 结构化文档方案, 数据存储采用关系数据库。

### 2.2 集成化IETM系统的功能

#### 2.2.1 技术信息查询

技术信息查询是 IETM 的主要功能, 在集成化 IETM 系统中同样具有, 主要实现对各种技术文件的查询、浏览功能。技术信息包括装备维修过程中涉及的修理工艺、零件鉴定和质量检验等信息。查询方式包括按结构展开、按关键词索引和按内容索引等。查询结果以文本、原理结构图和视频动画等形式显示。

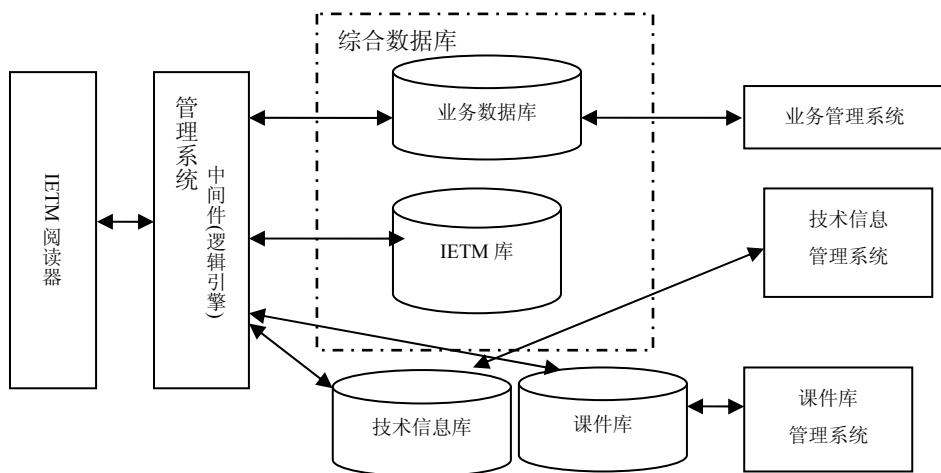


图1 集成化 IETM 系统总体结构

### 2.2.2 业务处理

传统 IETM 的交互性体现在查阅电子文档时，用户输入信息和显示结果之间的交换，即根据用户的输入显示相应的知识点。而集成化 IETM 的基本特征是实现技术信息和业务信息的交互，能够根据技术条件参数和实际情况进行业务处理。例如在装备修理过程中需要进行零件鉴定，用户根据鉴定零件的种类查询鉴定技术条件（包括：免修极限描述、免修尺寸、配合件、处理方法等）来决定该零件是修复、报废还是堪用。传统的 IETM 只给用户提供参考信息，不能接收鉴定结果。集成化 IETM 具有输入鉴定结果的接口，并能和其他业务集成，对报废处理的结果产生器材请领单，对修复处理的结果产生待修件信息，为制订修复计划提高依据，从而实现修理过程的交互。

### 2.2.3 智能诊断

修理技术文件是一种规范性标准文件，通用性强，无法满足具体装备修理过程中的个性化需求。集成化 IETM 系统通过将业务数据和技术标准数据的交互，能够解决这一问题。通过装备修理前采集的装备状态信息，系统能够应用智能库的知识进行判断，自动形成单一装备的修理方案；能够根据各种部件检测设备采集的数据，自动形成部件修理建议，从而提高了装备修理效率和准确程度。

## 3 系统实现的关键技术

### 3.1 技术信息的分类与重组

对技术信息重组是实现集成化 IETM 系统的一

个重要的认识。以前的技术信息是按章段节的方式进行组织的，这种方式不利于灵活的组织整体的信息。采用面向对象的方式来处理技术信息，将技术信息按一定的方式进行分类，重新组织技术信息，使之更有利于数字化管理。技术信息分类是以某种主题为出发点，对事物进行描述。装备维修保障的信息主要用途是指导维修人员进行维修保障活动。基于维修活动向量空间将技术信息分成互不相交的各类是一种可以尝试的方法。

向量空间模型（Vector Space Model，VSM）中，将分类对象看做是由相互独立的元素（ $T_1, T_2, \dots, T_n$ ）构成，对于每一分类元属性  $T_i$ ，都根据其在分类对象中的重要性程度赋予一定的权值  $W_i$ ，并将  $T_1, T_2, \dots, T_n$  看成一个  $n$  维坐标中的坐标轴， $W_1, W_2, \dots, W_n$  为对应的坐标值，这样由（ $T_1, T_2, \dots, T_n$ ）分解而得的正交元属性矢量就张成了一个向量空间，分类对象则映射成为空间中的一个点，对于所有元组和类都可映射到此分类向量空间。用元属性矢量（ $T_1, W_1; T_2, W_2; \dots; T_n, W_n$ ）来表示，则将对象类的匹配问题转化为向量空间中的向量匹配问题<sup>[3]</sup>。维修活动按时间顺序分为：功能的描述、操作方式、保养说明、检查、故障报告、分解、修复、组装、存储、其他几类向量。由于这些内容是在时间维上进行的，它们之间是正交的，而维修技术信息是对维修活动的描述，因此，二者向量的匹配应当是大致吻合。因此，技术信息可基于维修向量空间分类为下面几种类型：人员岗位信息、功能描述信息、故障诊断信息、零部件信息、预防性维修信息、紧急情况处理信息、线路图信息。

根据向量空间的分类,将集成化 IETM 系统的数据分成一个个数据模块,这个数据模块就包含技术信息中的最小单位。通过对这些数据模块的重组来表现完整的技术手册中的信息。

### 3.2 技术信息的描述方式

集成化 IETM 系统需要采用标准的和中性的方式来描述信息,只有这样才能实现数据本身与显示的分离。达到不管显示的方式如何,可以单独地对数据进行简单和安全维护的目的。根据目前的技术条件,可以考虑在系统发布和信息交换时需要采用 XML 标记语言作为载体。集成化 IETM 的另一重要特性是互用性和共享性。XML 具有的可扩展性、交互性好、高结构化、内容与显示分开的优点都可以满足这些要求<sup>[5]</sup>。

使用 XML 描述技术信息的关键是进行技术信息的文档类型定义 (DTD) 或者是 schema。通常情况下,DTD (schema) 列出了可用在文档中的元素、属性、实体和符号表示法,以及这些内容之间可能的相互关系,指定文档结构的一系列规则。因此,可以将 IETM 技术数据层次结构映射为 DTD 文档。这些 DTD 结构的构建不仅要考虑使用过程中功能的需要,如检索、导航、定位。还要考虑数据库存储问题、技术信息显示时的样式问题。需要将这些问题都反映在 DTD 结构中。由于这些问题在我国还没有相关的标准,需要参照相关的外军标准,但必须根据装备维修的实际情况对 DTD 结构进行剪裁。

### 3.3 集成化 IETM 系统界面的管理

集成化 IETM 系统是一个电子显示系统。虽然它可以存储大量的技术信息,但是在屏幕上显示的空间却是有限的。这是当前计算机自身无法克服的一对矛盾。也就是,当利用计算机存储大量技术信息时,尺度有限的屏幕无法显示信息的整体情况,即便是技术信息有重点的显示,屏幕也常常是

参考文献 (略)

#### 作者联系方式

通信地址:北京市丰台区杜家坎 21 号装甲兵工程学院技术保障工程系

邮政编码:100072

联系电话:010-66719453

捉襟见肘。这种问题的存在就需要对界面进行优化显示,弱化矛盾。与此同时,人的生理以及人脑的认知过程也是有特点的。如何根据人的特点,让计算机屏幕以最优的方式显示 IETM 的内容,成为 IETM 设计时应考虑的一项重要内容。以人的认知特性为约束,以界面显示的要素为变量,对界面进行组织,力使 IETM 在最大程度上满足使用人员的要求<sup>[6]</sup>。

通过参考认知学理论以及技术信息使用的功能,提出几项原则。

同一个系统内建立链接的标准要一致。保证操作人员能够根据标准清楚地掌握链接的路径,防止操作人员按链接寻找信息时发生“迷路”。

系统界面中的每一个链接要含意准确。建立统一的定义、程序,防止形成的链接节点在其内容上语义不同,最后与用户的预期不符。

界面中的链接要完备。同样要对信息的定义、程序等内容进行分析,尽量发现语义相近的内容之间的链接;同时,还应当适当控制链接的数量,以减轻用户的认知负荷。

总之,集成化 IETM 系统要有一个与用户十分贴切的界面。这是由人类心理和思考问题的复杂性造成的。但是人也有通过学习接受不同事物的能力,正是有这种能力,才值得我们科学地规划集成化 IETM 系统的界面,使系统易于操作和使用。

## 4 结论

当前,随着我军装备保障信息化建设的开展,各军兵种都已对现有装备实施信息化改造,在技术资源方面,对技术资料内容的规范、数字化制作与应用以及 IETM 系统都提出了急切需求。本文不仅要从技术可行性考虑,还要从我军的实际情况出发,分析了装备技术保障信息集成化 IETM 系统建设的几个问题,对提高装备信息化的集成度提供了参考。

# 浅谈信息化联合作战条件下的通信系统组织

毕国平 王作鼎 戴鑫焱

**摘 要：**信息化联合作战条件下的通信系统组织，必须以实战为牵引，紧紧抓住信息化联合作战的主要特点及其对通信系统的全新要求，从平台构建、网络组织、系统控制、力量运用和资源管理等方面综合考虑，全面筹划。

**关键词：**信息化；联合作战；通信系统

未来信息化条件下的联合作战中，通信系统作为实现诸军兵种一体化的桥梁和纽带，地位关键，作用突出，必然具有与机械化战争时代通信系统不同的特点和要求，同时也对系统的组织和运用提出了新的挑战。

## 1 信息化条件下的联合作战对通信系统的全新要求

### 1.1 高效可靠、互联互通

信息化条件下的联合作战，参战力量多元，各种武器云集，军、兵种间的相互支援和配合，不仅体现在联合战役的全局层次，也渗透到下级战役军团以至战术单元的作战行动之中。通信系统是将各作战要素、作战平台和武器装备系统有机地结合成一个整体，保障作战指挥控制及时、高效、稳定和实现战场信息高度实时共享，迅速把信息优势转化为决策优势和行动优势，夺取战争胜利的关键。因此，信息化联合作战条件下，通信系统组织必须打破军兵种自我保障的传统模式，从战役全局出发，强化综合意识，树立系统观念，建立纵向贯通、横向融合、各军兵种互联互通的通信网络，实现各军兵种通信系统的一体化。

### 1.2 全面组织、立体覆盖

随着以信息技术为基础的高新技术武器装备的大量使用，信息化条件下的联合作战将在陆、海、空、天、电磁多维战场空间同时进行，其力量部署呈现高度分散和立体化特征；分布于战场广阔立体空间的各作战单元、武器平台、力量要素围绕着同一作战目标协调一致的行动；作战指挥、作战行

动、火力运用、作战保障等在各个作战层次、作战阶段高度一体化。这一特点，要求通信组织必须综合运用各种通信手段，统一协调全部通信资源；通信系统必须覆盖战场的每个角落、每个作战单元，具有联通三军和全维作战空间的能力，确保多军种参战力量能够发挥整体作战效能，实现三军一体化作战目标。

### 1.3 快速反应、整体联动

信息化联合作战条件下，敌我双方将利用各种侦测设备，对己方和对方的作战行动进行全时空和全频段的侦察控制，战场透明度高，双方都需要通过灵活多变的战术和快速的机动来掌握作战主动权。因此，在一体化联合战场上，各作战单元将围绕同一作战意图，以“非线式”作战代替“线式”作战，强调在运动中完成作战部署，在机动中创造有利态势，注重以运动夺主动，以机动求生存。面对瞬息万变的战场，稍纵即逝的战机，通信系统只有快速反应，整体联动，对各类信息做到实时接收、传递和处理，才能为各作战单元实施无间断的机动作战提供可靠的通信保障。

### 1.4 整体防护、抗毁抗扰

在信息化条件下的联合作战中，为争夺制信息权，作为信息系统核心的通信系统必然成为敌方干扰和破坏的首要目标。未来战场上，在不能保证先机制敌、快速致胜的情况下，面对强敌的立体侦察、全频干扰和精确打击，通信系统能否经得住不间断的软杀伤和硬摧毁，将成为我军取胜的关键。因此，我们在不断提高通信装备技战术水平的同时，必须科学组织通信系统，改变以往各自为战的防护模式，确立“体系防护”观念；同时，还应从

系统的结构入手,合理配置,科学布局,使信息化条件下的联合作战通信系统具备灵活多变的抗毁抗扰和生存能力,实现稳定、可靠、不间断的信息传输。

## 2 信息化联合作战条件下通信系统组织运用对策

### 2.1 构建全维一体的通信平台

在信息化条件下的联合作战中,面对多维的战场空间和分散的力量配置,作为实现各作战平台和作战力量融合、形成作战体系的桥梁和纽带,通信系统必须覆盖战场的每个角落,构建全维一体的通信平台。

首先,立足各维空间,建立通信平台。综合利用作战区域内既设的军民光缆线路、固定短波台站、卫星地面站等各类通信设施,构建覆盖面广、纵横一体的陆基固定通信平台;综合使用微波接力、卫星、无线电双工移动等多种传输和群路交换设备,构建具有综合接入、综合传输和综合交换能力的一体化陆基机动通信平台;在海军舰船或民用商船上,分别配置野战综合数字交换机、短波自适应跳频电台、群路卫星通信等设备,组成海上通信平台;利用直升机和系留气球作载体,把无线电转信、中继和交换设备升至空中,构建空中通信平台;有效利用战略、战术通信卫星,构建覆盖整个作战地域的太空通信平台。

其次,运用多种手段,实现平台一体。信息化战场上,各类通信平台的覆盖范围不同,保障方式各异,既有自己的优势,也有各自的不足。通信系统的组织,必须把各类通信平台联为一体,互为补充,互为手段,形成覆盖全维、互联互通的平台网络,才能满足联合作战的需要。因此,我们要综合运用光纤、卫星、散射、接力等多种手段,采用统一的信令、协议、标准,通过交换机互连、无线中继、电台转信、网关接入等多种方式,达成各个平台间的远程、宽带互连,保证处于战场上任何位置的用户,都能够通过最近的平台入,与其他通信平台的用户实现信息互通。

### 2.2 组织各网一体的通信网络

三军一体化组网。首先要统一技术体制和标

准。制定具有前瞻性、先进性、权威性和开放性的技术体制和标准,无论是新装备的开发,还是老装备的改造,都必须严格按照统一技术体制和标准实行,为实现三军一体化通信组网提供物质基础。其次要统一系统软件。我们应按照通用化、系统化、标准化的要求,大力开发通信装备和网络应用软件,构建起相应配套的作战应用软件体系,利用功能强大的软件平台,实现不同网系之间的互通互操作,以提高系统综合组网的水平。再次,要根据联合作战任务,打破军种界限,按照统一计划、分级组织、网络布势、区域保障的要求,以光纤、卫星、短波通信为主,综合运用各种通信手段建立覆盖整个作战地域的一体化通信网络。

野固一体化组网。首先要抓好固定通信设施建设。在整体规划上,着眼作战需求,从有利于发挥固定通信设施最大作战效能,有利于与其他通信系统互联互通出发。同时,按统一的技术体制和网络协议改造现有固定通信设施,确保各通信基础设施互联互通;开发通用的网关和接口系统,便于固定通信网络的拓展和各野战通信系统的接入。其次在组织运用上,要综合运用有、无线通信手段,利用作战区域内的交换中心、通信枢纽和其他各类通信设施,建立一个诸军兵种共享、传输方式多样、传输路径多路迂回的野固一体化通信网络,实现指挥控制、预警探测、情报侦察等信息的实时传输。

军民一体化组网。我国民用通信资源丰富,地方的光缆、移动等通信网络遍布全国各地,容量大,业务全,未来一体化联合作战通信保障应走军民结合之路。一要充分利用作战地区内既设的光纤、移动等民用通信设施,以军用野战和固定通信设施为依托,多路由迂回组网,建立起军民结合的一体化通信网络,实现军民业务交叉。二要完善国防信息动员机制,平时要搞好对地方信息资源的调查,制定各种情况下的军地联合通信保障方案,战时要根据信息动员计划,依法动员地方信息资源,统一组织军民一体的联合作战通信网络。三要完善军民联动机制。各级通信部门平时应加强对地方通信网络建设情况的了解,定期举行军地区域通信网络互通演练,保证民用通信设施在战时能快速、有效地转入军用体制。

### 2.3 实施三军一体的指挥控制

未来信息化条件下的联合作战,通信保障力量

众多,构建的通信网络系统点多、线长、面广,只有实施一体化的指挥控制,才能实现不同方向、不同空间、不同层次、不同类型通信力量快速、协调一致的行动,实现通信系统的快速反应和整体联动。

首先,要建立权威指挥机构。以适应信息化联合作战指挥体制为基点,建立以战区通信部门为基础,其他各军兵种、武警、预备役、民兵以及地方通信部门共同参加的联合作战通信指挥中心,负责统一领导联合作战中的通信网络组织。其次,要统一调配通信力量。建立由联合作战通信指挥机构至各军兵种通信指挥机构、主要通信部(分)队的指挥控制系统;集中编组参战部队的通信力量,统一协调分配作战地域内的军地通信资源;统一组织通信管理、防护和技术保障,实现各通信力量的有机结合,提升整体保障能力。再次,要统一建设公共网络。联合作战中,凡属涉及诸军兵种公用通信网络的组织事宜,应实行统一指挥,协同通信平台的组织,必要时也可实施越级指挥,确保协同通信顺畅。

### 3 信息化联合作战条件下通信系统组织应注意的几点问题

#### 3.1 强化网络资源管理

未来信息化联合作战,参战力量多元,战场空间广阔,各类战场信息都要经过通信系统在各作战单元之间不间断地传递,通信业务量激增,对网络资源的需求也呈指数级增长。为此,我们必须通过强化网络资源管理,提高资源的综合使用效益。一是组建专门的通信网络资源管理权威机构,配备具有网络管理、维护和协调能力的专业人才。二是理顺通信网络组织管理体制。在联指建立战区网络管理中心,负责整个作战区域通信网络运行状态的监测和信息流量的分析,以及异常状况的分析排除;按不同作战区域建立区域网络管理中心,负责本区域内通信网络业务的管理和协调。三是建立通信网络资源管理系统,对通信网络上运行的资源进行统一管理,并能自动进行资源动态调整,提高通信网

参考文献(略)

作者联系方式

通信地址:重庆通信学院研究生队

邮政编码:400035

联系电话:13228689755

络资源的综合利用率。

#### 3.2 合理编组通信力量

信息化条件下的联合作战,参战军兵种多,指挥协同复杂,通信任务转换频繁,投入的通信力量规模大、专业多,通信系统组织异常复杂。为此,我们应着眼发挥各自的优势,科学编成和运用参战的各类军地通信力量。一是统一计划,突出重点。在分配及编组通信力量时,应从全局考虑,在重点保障担负主要任务的部队和重要战斗环节的同时,尽可能满足整体保障的需要。二是跨军种编组,按任务编配。打破各级通信部队平时的编制界限,统一编组不同功能、不同样式的通信保障群,构成相互支援、编配多元、功能互补的通信力量体系。三是集中使用、灵活运用。将一体化联合作战各区域内的各种通信力量统一组织起来,灵活运用、协调配置,形成三军一体、军民结合的区域性保障群,同时掌握一定的通信预备队,确保在各个战场、各个方向具有相对独立、能够持续作战的通信保障能力。

#### 3.3 实施综合通信防护

军事通信系统是一把双刃剑,它在实现信息交流与共享方面具有无与伦比的功能,可一旦受损也将带来不可想象的灾难。因此,在通信系统的组织运用中,一要注重基础设施防护。加紧地下通信防护工程改造,对重要通信设施进行伪装,对主要通信要素进行电磁屏蔽。二要加强网络安全防护。除了安装防病毒软件和制定安全保障制度等常见的安全措施以外,应建立全程全网的整体安全理念,集成各种安全新技术。三要科学组织防护措施。组织通信联络时,在认真研究敌我通信对抗能力的基础上,熟练运用伪装、示假、佯动、多点多控等战术手段,充分利用自适应、跳频和数字保密等抗扰能力强的通信装备组网。四要组建专业防护力量。统一调度各种通信力量,建立一支专业的通信防护队伍。

# 信息化条件下我军武器装备信息化发展途径探讨

高小玲 卜格鸿 刘力天

**摘 要:** 本文通过对世界各国武器装备信息化的发展历程进行分析, 提出对信息化武器装备效能进行评估的方法, 最后对适应我国武器装备信息化发展的途径进行探讨。

**关键词:** 信息化武器装备; 信息技术

从 20 世纪末到本世纪初, 在世界范围内发生的局部战争越来越明确地说明, 掌握信息化就掌握了战争的主动权, 拥有信息化部队和信息化武器装备, 就拥有了战争的制胜点。由此可见, 武器装备的信息化正悄然引导着新军事变革。发展信息化武器装备, 既是军事变革的基本内容, 也是实现我军信息化建设目标的关键所在。

## 1 信息化武器装备的概念

信息化武器装备是相对于传统的机械化武器装备而言的, 它们之间的最大区别就在于, 前者是网络系统中的武器, 后者是单个武器平台。信息化武器装备, 指信息技术含量高、信息起主导作用的作战武器和保障装备, 主要包括军队的  $C^4ISR$  系统、信息化作战平台、智能化弹药、智能机器人、数字化单兵系统等。

由以上的概念可以看出, 军队要拥有信息化武器装备, 首先要立足于实现武器装备的信息化, 也就是指利用信息技术和计算机技术, 使预警探测、情报侦察、精确制导、火力打击、指挥控制、指挥调度、通信联络、战场管理等领域的信息采集、融合、处理、传输、显示, 实现自动化和实时化。武器装备信息化, 直接导致武器系统的智能化和作战系统的一体化。信息化武器装备的出现, 是信息技术、计算机技术、数据处理技术、空间技术, 以及新材料技术等高新技术, 作用于传统武器平台的必然结果。

## 2 世界各国武器装备信息化的发展途径

21 世纪初, 随着高新技术的迅猛发展及其在

军事领域的广泛应用, 武器装备在军事斗争和军队建设中的作用日益突出。因此, 世界各国为争取在下个世纪的战略主动权正在积极做准备, 实现武器装备的信息化便是各国不遗余力准备的重点。在实现武器装备信息化的过程中, 虽然各国的国情千差万别, 所采取的措施多种多样, 但其中也不乏共同性。

### 2.1 立足现有武器装备, 利用成熟技术横向集成

技术创新已不仅限于全面使用全新技术, 而且指成熟技术的系统化和集成化, 并以此改造现有武器装备或集成一种极富创新性的系统。利用成熟的技术将分立的武器装备或系统通过集成形成一个新的更高层次的系统, 可以大大提高现有武器装备群的信息化能力, 实现“ $1+1>2$ ”, 这种方法已经成为目前国际范围内武器装备“一体化”发展的新趋势。这样, 既可以提高现有武器装备的信息化程度, 又能够节省大量资金。因此, 越来越多的国家从以高投入建造大批新型武器装备转向利用成熟技术的集成化、系统化、一体化, 对现有武器装备改进或组合形成较新的武器装备, 这已成为今后相当长时期内世界武器装备发展的一种新举措。

### 2.2 加强军事技术引进, 联合生产信息化武器装备

军事技术的交流和引进是一种双赢策略。对于军事技术发达的国家来说, 可以缩短研制周期, 优势互补, 降低各自的风险与负担。加强军事技术引进和国际合作对军事相对落后的国家来说, 提高其研制起点, 缩小差距, 减少其盲目性; 可以获取先进的国防科研生产的管理经验, 提高本国军工部门



的技术和生产能力，为发展本国军事工业奠定基础。不过军事技术的引进需要大量的资金作保障，对于经济和军事实力均不强的国家而言，通过引进技术直接生产信息化装备这种做法并不现实。

### 2.3 利用新技术，研发新型信息化武器装备

研制新型信息化武器装备，用全新的设计思想和顶尖技术研发新装备，强化其探测、判断、识别、定位、打击、机动和隐形等综合功能，增加武器装备库中的“新生力量”。从20世纪90年代末开始，西方发达国家凭借其强大的经济和科技实力，把发展新型信息化武器装备作为军队转型的重要内容。

### 2.4 优化武器装备结构，由信息化牵动多元化

信息技术的发展及其在武器装备制造和改进中的应用，使得传统的作为主战力量之一的武器装备的作战性能产生了质的飞跃，其作战能力的提高已不仅仅依赖于机械性能的提高，而是转为多方面能力的全面提高。未来战争是陆、海、空、天、电五维一体化的战争，是大系统与大系统之间的对抗，这种体系对抗的特点要求武器装备的发展必须从强调几种主战装备，扩大为重视多种功能武器装备的协调发展；从单类武器装备的高性能，上升为着眼提高武器装备体系的整体质量与效能。如果只一味追求某类武器的发展或某项关键装备的发展，造成与其他能力的不匹配，就会影响其他功能的正常发挥，大大降低武器装备的整体效能。因此要强化体系观念，从作战体系的角度将武器装备发展作为一个系统工程，优化武器装备的体系结构，建立最佳配置体系，着眼于提高整个作战效能。

## 3 正确评估信息化武器装备的效能

探讨我军发展武器装备信息化的途径，首先必须搞清评估信息化装备的标准，即如何评估信息化装备的效能，在此基础上进一步研究既适合我军实情又能够最大程度发挥信息化装备效能的发展途径。

武器装备最终是为作战服务的，信息化武器装备的效能要在和平时期就能给出正确的评估，如果

只有在战时才能对效能做出评估，则为时已晚。

### 3.1 正确认识武器装备信息化

首先，武器装备信息化的目的不是演示而是作战，装备信息化建设的所有环节都要为作战目的服务。平时保证装备的作战性能和战时发挥装备的作战效能，永远是第一位的。其次，要挖掘装备的作战潜能。任何一种信息化装备定型后，其战术、技术指标，以及作战性能都是确定了的。通过科学管理，保持其战术技术指标，通过严格训练和保障，使其设计潜能得到最大释放，是使信息化装备的作战潜能转化为战场上的作战效能的关键。必须通过改革训法、用法，使装备的某些设计缺陷得到弥补，潜在优势得到扩张，最大限度地提升综合作战指标。第三，要发挥装备的制胜效能。高性能的装备有利于掌握主动，普通装备也并非无所作为。装备信息化建设的一个重要使命，就是保证部队用好手中的武器装备，扬长避短，立足现有条件加快现有武器的信息化改造，找到发挥自身优势、用现有装备战胜敌人的对策。

### 3.2 勇于检验武器装备信息化的效能

用战斗力的标准检验武器装备信息化。武器装备好不好，管不管用，能管多大用，只有到战场上方能定论。问题在于待到战场做出裁决时，一切都已无可挽回了。因此，必须在战前就有检验装备信息化建设效能的战斗力的标准。检验战斗力的标准有三个：一是动态标准。保持装备完好率、配套率仅仅是静态指标，装备最终要动起来，要做到人装结合。只有在人装结合后的各项指标才是动态标准，动态标准才能更真实地反映装备战术技术指标的本质，才能更接近战时装备保障的实际。二是系统标准。单台件装备、单项指标不足以反映装备全貌，必须成系统地看装备是否好用，系统是否配套，保障是否有力，一句话，看整体作战能力强不强。这里既涉及装备，也涉及人员，既有技术问题，也有战术问题。三是长远标准。检验装备信息化效能不看一时一域，而要看全面，看长远。只顾眼前不顾长远的短视行为，可能风光一时，但无法持久。衡量一支部队的装备信息化建设水平，在看到其现实能力的同时，还应看它的基础，看它的整体，特别是看它的发展潜力。

### 3.3 按照实战标准不断推进武器装备信息化的程度

用战斗力的标准推进装备信息化。仗怎么打兵就怎么练,保障就怎么搞,以战斗力标准牵引装备信息化建设是基本导向。在装备信息化建设中落实战斗力标准,一要抓好重点建设。尤其在任务重、时间紧、财力有限的情况下,更要依据任务进行重点建设,突出重要方向和新型主战信息化装备的保障,突出装备指挥建设、战役保障力量建设和战场预置建设,突出老装备信息化改造、新型装备形成作战保障能力、武器平台与指挥平台的信息化链接。二要强化配套建设。单台件装备本身资料、附件、工具等技术配套很重要,但更要重视逐级逐步抓好各类信息化装备的系统配套、作战装备和保障装备的配套,以及人装结合能力和用修能力的综合配套。三要注重成建制建设。坚持成建制建设的思路和工作方法,逐步扩大现有装备信息化建设的规模,是实现装备信息化的必由之路。为确保部队能成建制地形成信息化条件下的作战能力,必须成建制地组织装备的模拟化和实战化训练,使建制内的各种装备形成与作战需求相适应的整体保障能力。

## 4 我军武器装备信息化可采取的主要途径探讨

我军处于后发之势,要想实现跨越,完成新时期的历史使命,而不是在发达国家后面尾随或跟进,就不能不从自己的国情军情出发,先思而后动,在借鉴和扬弃的基础上,选准目标,走出自己的路。这条发展道路应该是:以未来作战需求为牵引,以满足国家安全需求为目的,借鉴发达国家有益做法,立足国内,自主创新,充分吸收和运用地方已有的信息技术成果,开发与改造并重、信息化战场环境建设与武器装备的信息化平台建设和改造并重,软硬件建设兼顾,突出重点,形成具有中国特色的“复合式”发展道路。

### 4.1 立足国内,自主创新,用创新技术加速发展我军武器装备信息化建设

理论创新是技术创新的先导。根据我国和我军

的实际情况,在现阶段应立足国内,自主创新,以理论创新牵引技术创新。首先,应加强对武器装备发展趋势的预测与预研,特别是对新概念、新机理武器的研究和预测,为武器装备的发展提供理论基础和技术基础。其次,研究世界范围内的军事变革和近几年发生的局部战场,把握世界军事变革的趋势,明确未来战争对武器装备的基本需求,正确把握武器装备发展的大方向。第三,应以作战需求牵引理论研究,科学论证武器装备建设的发展战略和长远规划,优化装备体系结构,使武器装备与未来军事斗争的要求相适应,与国家经济、科技发展水平相适应。第四,在自主创新的过程中,抢占技术创新的制高点。现代高新技术是以信息技术为核心的一批高技术群,技术创新面临着众多课题。推进中国特色军事变革,必须准确把握世界高新技术发展的特点和趋势,高度关注对军事变革有重大影响的技术创新重点领域。

### 4.2 以重点突破,局部跃升带动武器装备信息化整体提高

研制新型装备需要花费大量资金,耗费巨大的人力和物力,甚至对于美国这样的经济大国也感到难以承受。而且新型装备在短时间内难以形成战斗力,也不可能一下子更换所有的旧式装备。所以在大力研制和开发新型武器装备的同时,不应忽视对仍有潜力的老式武器装备的改进,特别是对一些具有典型代表性和广泛应用的重点装备的改造,通过对这些重点装备改造的突破,以信息技术手段带动武器装备信息化整体水平的提高。

在武器装备的改进中大量采用信息技术,已被实践证明是一条行之有效的发展道路,既可在短时间内提高武器装备的作战效能,又能节省大量研制经费,所以应予特别重视,确保这方面人力和经费的投入。同时在发展新型号的飞机、坦克、舰艇、火炮等传统概念的武器装备时,也应采用计算机辅助设计、计算机模拟等信息技术手段进行研制,以求达到最少的投入、最短的时间和最佳的研制效果;并在设计之初就把武器装备的探测、传输、处理、控制、安全、对抗、显示、兼容、一体化等信息性能放在优先地位,以求达到信息化条件下武器装备的最优作战效能。

### 4.3 推行模块化思想，提升武器装备信息化能力

随着微电子和计算机辅助设计等技术的发展，武器装备设计水平日趋成熟，表现在其发展的有序化和系统工程的较高的管理水平，从而大大推动了武器装备的通用化、系列化、模块化建设。武器装备建设实现了这“三化”，则可极大地缓解经费不足，缩短研制周期，保持高技术装备发展的势头，满足未来战争联合作战的需要，在经济上、技术上和战术上都具有长远的战略意义。

### 4.4 加强人才培养，为技术创新提供可靠保证

建设信息化军队、打赢信息化战争，迫切需要一大批高素质新型军事人才。人才是第一资源，人才优势是技术创新最根本的优势。人才是科技进步和经济社会发展的最重要资源，创新的关键在人才。要高度重视人才问题，始终要把人才建设作为创新的重中之重。目前，我军武器装备的发展正处于关键时期，研制发展信息化武器装备任重而道

远，更需要加快高素质、高水平技术人才的培养。我们既要充分发挥老一代科学家和科技人员的作用，搞好传帮带，又要采取各种有效措施，加快培养和造就一批具有追踪世界科技发展前沿、富有创新精神的年轻科学家和工程技术专家，形成技术创新的人才群体，为信息化武器装备的跨越式发展奠定坚实的人才基础。

另一方面，在实现武器装备信息化的同时，只有加强人才培养，才能按照实战的标准，努力实现人与武器装备的最佳结合，发挥信息化装备的整体优势和合力，提高信息化装备的整体效益。

## 5 结束语

我军要在未来战争中立于不败之地，首先必须建设一支由具有综合保障能力的信息化武器装备武装的信息化部队，而实现武器装备的信息化道路必须符合我国、我军的实情，只有分析现实、勇于创新、不断探索才能找到适合我军建设信息化部队的最佳途径。

### 参考文献

- [1] 朱幼文, 冯毅, 徐德池. 高技术条件下的信息战 [M]. 北京: 军事科学出版社, 2004
- [2] 赵可铭. 世界军事形势分析[M]. 北京: 国防大学出版社, 2001
- [3] 黄招强. 信息时代的战争形态浅析[D]. 北京: 国防大学, 2005
- [4] 俞晓鹏. 21 世纪战争趋势[M]. 北京: 新华出版社, 2002

### 作者联系方式

通信地址: 北京怀柔 3380 信箱 13 号装备指挥技术学院

邮政编码: 101416

联系电话: 010-66364259

# 基于复合Agent的信息系统模型设计实现

郭天杰 李瑛 范洪达

**摘 要:** 为了有效简化信息系统中软件组件以及物理设备组件的分割造成的网络管理问题, 分析提出基于复合 Agent 的分布式结构模型, 证明该设计可降低网络管理复杂度, 提高整个系统的自适应、自组织特性, 并易于集成和扩展。

**关键词:** 分布式系统; 复合 Agent; 自组织

## 引言

网络管理系统作为信息系统的重要组成部分, 是保证系统高效、可靠、经济和安全运行的重要支撑<sup>[1]</sup>。随着网络技术的发展, 网络规模不断扩大, 网络结构日益复杂, 处理的数据量不断增大, 基于 Agent 的分布式网络管理技术得到广泛的研究, 实验证明, 利用 Agent 技术能有效提高数据采集、处理的效率<sup>[2]</sup>。

在现代信息系统中, 网络管理的对象, 从传统的物理设备转变为基于小型机的软件子系统, 网络管理对象的分割方式和逻辑发生很大的变化, 网络管理需要同时兼顾基于逻辑面的软件组件的分割和基于物理面的设备组件分割策略<sup>[3]</sup>, 并要求在一定程度上满足 Agent 软件研究方向中的自组织和可扩展的发展方向<sup>[4]</sup>。通过复合 Agent 与子系统 Agent 结合的方式, 融合组件技术和适当的设计模式, 能够有效的适应分割策略的变化和灵活部署的需要, 同时也为基于软件子系统分割的模式提供良好的扩展性支持。使得系统能够在更高的层面上达到自组织、自适应和可扩展。

## 1 基于复合Agent的分布式网管模型

基于复合 Agent 的分布式网络管理模型如图 1 所示, 其中管理层可使用基于 SNMP 的标准协议对网络所有网元进行管理, 负责发出各种管理的请求和提供管理服务; 复合 Agent 层基于主机系统, 一方面负责接受和应答管理层发出的请求和服务, 另一方面将把 SNMP 协议的请求, 转化为主机设备内部进程间的控制和服务请求; 子系统 Agent 驻

留在软件子系统内部的, 用于具体处理管理层发出的控制和管理请求。

### 1.1 管理层

管理层通过三种方式实现网络管理功能: 一是通过 SNMP 操作直接与被管理对象代理交互, 以获得网元的即时信息或对网元进行远程配置管理; 二是通过对数据库的访问, 获取网元的初始配置和网元系统的历史信息, 以了解网元的历史状态; 三是通过数据分析系统, 对现有收集的网元数据进行分析和判断, 以提供对网元的优化和监控分析报告。管理层与复合 Agent 层之间的通讯协议是比较简单的, 通常使用 SNMP 协议来通讯。在较大规模网络中, 可按照管理域分隔管理层, 不同管理域之间不进行复杂的交互。

### 1.2 复合Agent层

复合 Agent 层基于主机设计, 包含一个自适应的、高度可扩展的代理容器和一组能够和子系统代理通讯的 Agent 组件。复合 Agent 对外通过 SNMP 协议连接网管中心, 对内采用进程间的 Agent 通讯协议, 与子系统中的 Agent 进行有效地即时通讯。

复合 Agent 设计成良好的容器型框架, 要管理的软件子系统看成是一个可自由出入的软件组件, 子系统在主机上的部署变化只反映为软件组件的配置变化。当需要增加或者减少某个软件子系统的网管时, 只需要较简单的软件组件配置, 即可使代理容器立刻识别新的管理对象的状态。复合 Agent 在设计上充分考虑对应用实体的状态控制和统计、配置管理、监控管理、系统报警等环节的支持, 因此用户能够非常简单地将原有固化在应用程序中的网

管部分移植到服务 Agent 的框架下。

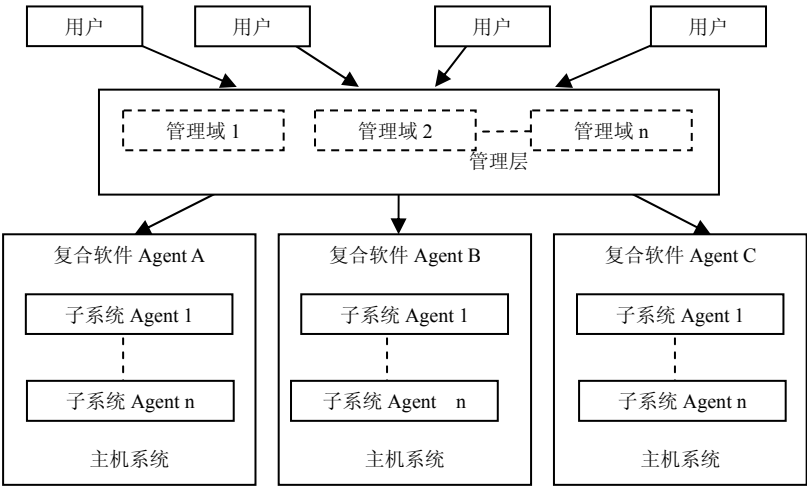


图 1 基于复合 Agent 的分布式网络管理模型

1.3 子系统Agent层

子系统 Agent 层嵌入在应用系统内部，负责收集应用系统的相关统计数据，发出指令给应用系统。复合 Agent 层的存在，不需考虑子系统 Agent 与远端的网络管理中心的通讯问题，子系统 Agent 可以设计得非常简单。在主机内部通讯比较简单，协议和管理方面就可相对简化，因此采用复合 Agent 层加子系统 Agent 的方式可以简化软件子系统的网管开发量，降低网元在网管上的资源消耗。

子系统 Agent 采用基类封装的形式，封装与复合 Agent 层进行进程间通讯的协议以及对网元的子系统进行网管管理的框架。在进程间通讯协议方面，利用消息队列，共享内存等通讯方式，灵活处理状态统计和命令控制两类网管指令。同时在网元子系统的管理框架方面，子系统代理的服务类，也提供了对网元子系统的状态统计，配置管理，命令控制，报警等方面的封装。

2 复合Agent层设计实现

2.1 容器部分

代理容器在复合 Agent 层中是一个自适应的、高度可扩展的模块，是所有 Agent 组件的管理者，负责驱动其内部的不同 Agent 组件，通过复合 Agent 通讯协议 AAP 来实现对各子系统代理的管理。代理容器、Agent 组件以及子系统代理之间的

关系如图 2 所示：Agent 组件设计成一个能动态加载的可执行链接库，复合 Agent 在启动时，代理容器通过读取相应配置文件知道需要加载的 Agent 组件，以及这些 Agent 组件的库文件存放路径和配置信息。然后代理容器依次动态加载 Agent 组件的可执行链接库，并调用各 Agent 组件的注册函数初始化各组件。复合 Agent 的功能是由代理容器来实现的，主要包括下列功能：

配置文件下载：复合 Agent 在启动后通过特定消息请求 NMS，并等待 NMS 应答配置文件所在的目录，然后由复合 Agent 去通过 FTP 的方式去下载这些配置文件到本地目录中。

动态配置：对于已经利用下载下来的配置文件启动了的应用实体，NMS 还可以通过动态修改的方式修改配置文件内的记录，并马上作用到应用实体中。

应用状态查看：NMS 可以通过 SNMP 请求来获取应用的当前状态，应用名称、启动时间、进程 ID 等等。

应用统计：NMS 可以通过 SNMP 请求来获取某一项业务的统计数据。

应用控制：NMS 可以通过 SNMP 请求来控制应用实体的行为，例如：启动、挂起、恢复、退出等等。

告警管理：当应用实体运行时出现了一些紧急的状况需要通过 NMS 报告给管理员时，会通过告警请求来完成。

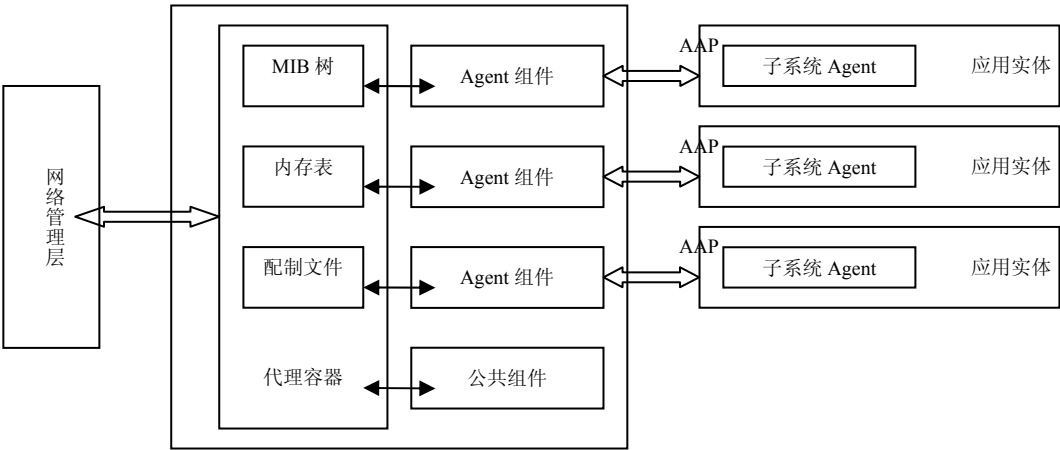


图 2 复合 Agent 层设计实现

2.2 Agent组件部分

Agent 组件是一组能动态加载的可执行链接库，为每一个 Agent 组件的动态连接库定义一个具有如下命名规则的注册和注销函数：

注册函数名称=[Agent 组件名称]\_LibInit

注销函数名称=[Agent 组件名称]\_LibFree

当代理容器需要加载某一个 Agent 组件时，可以通过该命名规则访问到注册函数，并调用该注册函数创建 Agent 组件对象，最后将 Agent 组件对象的句柄返回给代理容器以供以后调用；同样的方式，调用注销函数来释放 Agent 组件中已创建的系统资源。对于已经加载到代理容器的 Agent 组件，可提供初始化和销毁组件对象、空闲处理、查询应用状态、接收握手消息、应答握手消息、查询 MIB 表节点、动态修改 MIB 表节点等接口供代理容器使用。

2.3 复合Agent通信协议

复合 Agent 与应用实体之间的交互实际由 Agent 组件和子系统代理部分来完成，每一种复合 Agent 与应用实体之间的消息都定义了一个消息类型，复合 Agent 或子系统代理将根据约定好的格式进行解析。按这种消息格式进行解析的通讯方式命名为复合 Agent 通信协议 AAP。AAP 既可以承载在 TCP/IP 上，也可以承载在 IPC 消息队列通讯上。

参考文献（略）

作者联系方式

通信地址：山东烟台二马路 188 号海军航空工程学院 205      邮政编码：264001      联系电话：0535—6635593

2.4 子系统代理部分

子系统代理部分设计成一个模块对象类，应用继承该模块对象的事件处理函数，由应用实体实现其网管功能。该模块对象被划分为两部分，一部分为代理适配器通讯模块，负责与复合 Agent 进行 IPC 消息队列通讯，通讯协议采用复合 Agent 通讯协议；另一部分为代理适配器模块，负责与上层应用交互，并驱动上层应用的相应功能函数。

代理适配器通讯模块对代理适配器提供发送和接收数据的接口，代理适配器不受代理适配器通讯模块与复合 Agent 进行通讯方式的影响，所以在实现代理适配器通讯模块时可以任意选择底层的通讯方式。

3 结论

基于复合 Agent 的分布式网络管理模型，在开发基于软交换技术的软件组件网管系统中发挥了重要的作用，系统能够实现对软件子系统的高效管理，有效地支持软件子系统的灵活部署和自由扩展。复合 Agent 可进一步发展与其他复合 Agent 协商，完成特定任务，向更加智能化发展，支持负载均衡提供更好的系统稳定性；复合 Agent 与子系统 Agent，以及子系统 Agent 和应用子系统之间的协议也将发展的更加完善，使得通信协议能够更加有效地按需配置，达到最优性能价格比。

# 一种通用的基于元数据的异构数据库数据移植技术

蒋国权 严浩 刁兴春 汪挺

**摘 要：**如何实现异构数据库间的数据移植是企业信息化建设面临的巨大挑战。在分析传统移植方式的基础上，对 Oracle 的系统视图、SQL Server 的系统表进行了探讨，提出了一种采用 Access 中间库、基于元数据、库表结构和数据分离的数据移植方式，为企业的综合信息系统数据集成提供了一种技术途径。

**关键词：**元数据；异构数据库；系统视图

## 1 引言

在信息系统的发展初期，企业各部门建立了众多相互独立的数据库应用系统。随着这些应用程序的推广应用，积累了大量的宝贵数据，这些数据是企业信息化建设的巨大成果和财富，是企业下一步信息化建设的数据基础。但是由于这些数据库系统在前期的规划、设计、开发阶段中，往往局限在特定的使用单位和用户范围，没有考虑数据的可移植性。因此，在企业内部形成了众多的异构数据库系统，这种异构数据并存的局面，导致了数据移植的巨大困难，造成数据利用率低，无法发挥更大的作用。

企业的现代管理对企业的信息化建设提出了新的要求，需要整合原来不同部门的数据，对数据进行综合分析，从而提取出有用的信息。如何有效合

理地对原来的各部门的信息系统进行集成，使得企业的信息化建设平稳地过渡到综合统一的信息系统新阶段，是摆在我们面前的一个迫切需要解决的难题。由于数据库系统在各种信息管理系统中都处于核心地位，如果异构数据库的一体化难题得不到解决，企业综合信息系统将面临无米之炊的尴尬局面，也是企业综合信息系统能否取得实效的关键因素之一。本文根据企业综合信息系统建设的需求，结合工程的实际，设计并实现了一种基于元数据的异构数据库数据移植方案。

## 2 传统的移植方式

如何在异构数据库之间进行数据移植，这是整合企业各部门信息系统时常常遇到一个技术难题，图 1 列出了传统的三种解决方式。

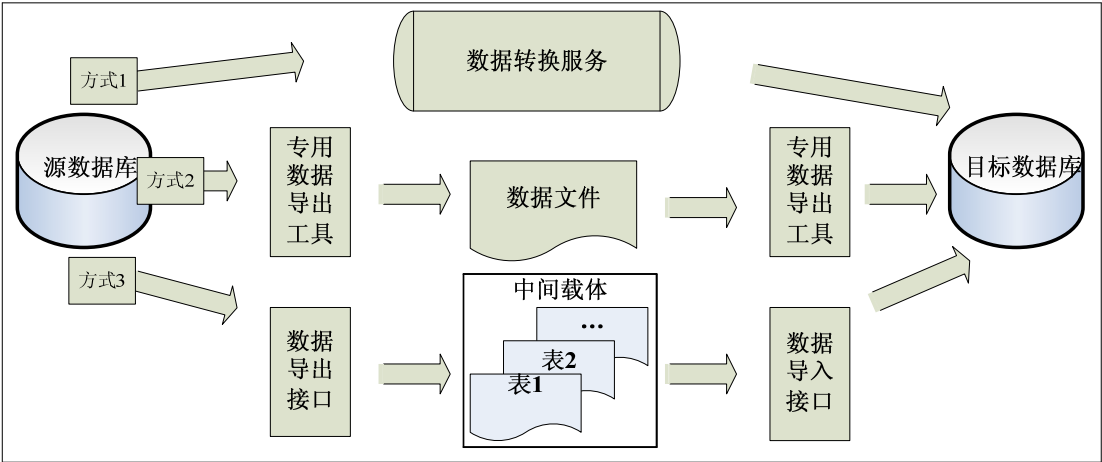


图 1 三种传统的数据移植方式



方式 1 是直接通过某些数据库系统自身提供的数据库转换服务来进行异构数据库之间的数据移植。这种方式的优点就是简单方便，不需要用户进行专门的应用开发。其缺点主要有两点。

1) 其支持的数据库类型受限，并不是每一种数据库系统都提供这种服务，即使提供了该服务，也往往带有诸多限制，不具有通用性。例如 SQL Server 提供的数据库转换服务<sup>[1]</sup>只能把数据从一个非 SQL Server（例如 Access 和 Oracle）传输到 SQL Server 数据库中，无法进行逆向的移植。

2) 往往需要源数据库和目的数据库之间能够进行网络通信。由于网络的问题或者从安全保密的角度考虑，在某些特定的应用场合将无法使用该方式进行数据的移植。

方式 2 主要适用于某些不同版本的数据库系统之间的数据移植。例如 Oracle 就提供专用的数据导出工具 EXP 和专用的数据导入工具 IMP 用来进行数据的导入导出<sup>[2]</sup>。这种方式的优点也是简单方便，对用户透明。其缺点主要是：只能用于同一类型的数据库之间的数据移植，即使在同一数据库类型中，往往只能用于从低版本的数据库移植数据到高版本的数据库中，应用范围受限。例如从 Oracle9i 导出的 DMP 数据文件就无法通过 IMP 工具导入到 Oracle8i 的数据库中。

方式 3 是用户开发专用工具，以中间载体的形式进行数据移植，中间载体可以是文本、Excel 电子表格、XML 文档<sup>[3]</sup>，用来保存从源数据库导出的数据。这种方式的优点是应用范围广，不受数据

库系统的限制。缺点主要如下。

1) 效率低。由于这些中间载体的很少用在数据库移植这种大数据量的场合，在大数据量的情况下，数据移植的速度和数据量的大小往往难以满足用户的需求。

2) 适应性弱。传统的移植方式体现了原表——中间表——新表的移植思路，开发人员需要理解分析每张表的结构定义，工作量很大。一旦需要转换新的库表，又要重新开发新的移植工具，极大地浪费了时间和人力。

3) 安全性差。文本、Excel 电子表格、XML 文档等中间载体往往缺少相关的安全保密措施，在中间载体的传输过程中缺少相关的安全保密措施和手段。

### 3 基于元数据的数据移植方案

本文根据企业综合信息系统建设的需求，结合工程的实际，设计并实现了一种基于元数据、数据和定义分离的异构数据库数据移植方案，如图 2 所示。数据字典是关于数据描述信息的一个特殊数据库。它包含每一数据类型名字、意义、描述、来源、格式、用途以及它与其他数据的联系等数据。这类数据称为元数据（meta data）。因而，数据字典又称为元数据库。系统从源数据库的数据字典中导出库表的结构定义，与库表的数据一起打包供导入使用。

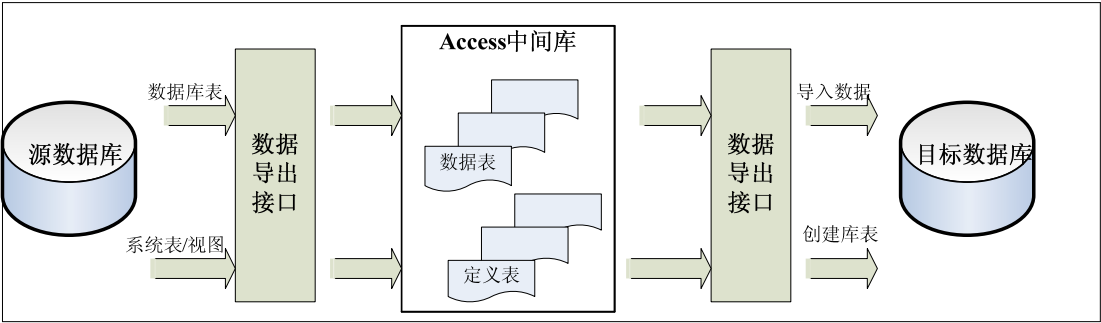


图 2 数据与定义分离的移植方式

该方式具有以下优点：

1) 效率较高。Access 作为一种通用数据库，速度和性能也大大高于文本、Excel、XML 文档等中间载体，且容易发布，使用比较方便。目前 Access 的性能已经可以满足中小型系统的需求。

2) 适应性强。本方案在转换移植时没有采用

传统的原表——中间表——新表的三部曲，而是把库表的定义和数据分别导入导出，从而使得本系统的通用性得到了极大的扩展，能够适应各种不同的库表结构，而不必重新开发。

3) 安全性高。本方案采用 Access 中间库，可以方便的采用 Access 自身具有的安全保密功能，



如数据库密码机制和用户级安全机制等，从而提高数据移植的安全性。

4) 可操作性强：采用 Access 中间库，导出的数据还可以直接进行操作控制，另外系统在数据移植时还可以进行灵活的进度控制。

由于 Oracle 和 SQL Server 是目前企业广泛应用的两种数据库系统，下面就以这两种主流数据库为例进行说明。

## 4 移植规则的定义

### 4.1 Oracle系统视图

在 Oracle 的数据字典中可以从若干系统视图获取库表定义信息，主要包括表信息系统视图、字段信息系统视图、约束信息系统视图、注释信息系统视图、触发器信息系统视图。

表信息系统视图 `USER_TABLES`<sup>[4]</sup>包含了当前用户所有的所拥有的数据库表信息，主要字段包括：表名 `TABLE_NAME`、表的拥有者 `OWNER` 等。

字段信息系统视图 `USER_TAB_COLUMN`，包含了当前用户所拥有或者可访问的表的字段信息，主要字段包括：表名 `TABLE_NAME`、字段名 `COLUMN_NAME`、数据类型 `DATA_TYPE`、数据长度 `DATA_LENGTH`、数据精度 `DATA_PRECISION`、数据刻度 `DATA_SCALE`、是否可空 `NULLABLE`、字段序号 `COLUMN_ID` 等。

约束信息系统视图包括 `USER_CONSTRAINTS` 和 `USER_CONS_COLUMNS` 两个系统视图。其中 `USER_CONSTRAINTS` 包括约束拥有者 `OWNER`、约束名 `CONSTRAINT_NAME`、约束类型 `CONSTRAINT_TYPE`、表名 `TABLE_NAME`、外键引用表主键约束名 `R_CONSTRAINT_NAME` 等主要字段。`USER_CONS_COLUMNS` 包含了组成主外键约束的字段信息，包括拥有者 `OWNER`、约束名 `CONSTRAINT_NAME`、表名 `TABLE_NAME`、字段名 `COLUMN_NAME`、位置 `POSITION` 等主要字段。

注释信息系统视图包括 `USER_TAB_COMMENTS` 和 `USER_COL_COMMENTS` 两个系统视图。其中 `USER_TAB_COMMENTS` 包含表的注释信息，包括表名 `TABLE_NAME`、表的类型

`TABLE_TYPE`、注释 `COMMENTS` 等主要字段。`USER_COL_COMMENTS` 包含字段的注释信息，包括表名 `TABLE_NAME`、字段名 `COLUMN_NAME`、注释 `COMMENTS` 等主要字段。

触发器信息系统视图 `USER_TRIGGERS`：包含了当前用户所拥有的所有触发器信息，主要字段包括：触发器名 `TRIGGER_NAME`、表名 `TABLE_NAME`、触发器描述 `DESCRIPTION`、触发器主体 `TRIGGER_BODY` 等。

以上系统视图以“USER”代表当前用户所拥有的系统信息，同时数据库存在以“ALL”作为前缀的系统视图，代表所有数据库用户拥有的系统信息。

基于 Oracle 数据库使用的普遍性，系统在导出数据时参考了 Oracle 系统视图的设计，在 Access 中间库中也分别建立了表信息定义表、字段信息定义表、约束信息定义表、注释信息定义表、触发器信息定义表。在导出数据时首先把需要导出的库表定义导出到 Access 中的定义表中，然后导出数据表。由于数据库表的定义信息得到了单独保存，所有中间库数据表可以设计成简单的格式，表的约束和字段类型等都可以弱化处理。

### 4.2 SQL Server系统表

不同数据库系统的数据字典在内容上大致相同，但是在结构上有较大的区别。SQL Server 的系统表与 Oracle 的系统视图在格式上就存在较大区别。SQL Server 的系统表包括：系统对象表、系统字段表、系统索引表、系统索引键表、系统外键表等。

系统对象表 `Sysobjects`：保存了数据库中对象的信息，每个对象（约束、默认值、日志、规则、存储过程等）在表中占一行。主要字段包括：对象名 `name`、对象标识号 `Id`、对象类型 `xtype`、对象类型 `type` 等。

系统字段表 `Syscolumns`：每个表和视图中的每列在表中占一行，存储过程中的每个参数在表中也占一行。主要字段包括：列名或过程参数的名称 `name`、表对象标识号 `ID`、物理存储类型 `type`、小数位数 `scale`、精度级别 `prec`、是否允许空值 `isnullable` 等。

系统索引表 `sysindexes`：数据库中的每个索引和表在表中各占一行。主要字段包括：表对象标识

号 ID、索引标识号 indid、键的数目 keycnt 等。

系统索引键表 sysindexkeys：包含索引中的键或列的信息。主要字段包括：表对象标识号 id、索引标识号 indid、列标识号 colid、位置 keyno。

系统外键表 sysforeignkeys：包含关于表定义中的 FOREIGN KEY 约束的信息。主要字段包括：外键约束的标识号 constid、表对象标识号 fkeyid、外键引用表对象标识号 rkeyid、正在引用的列标识号 fkey、已引用的列标识号 rkey、该列在引用列列表中的位置 keyno。

4.3 数据类型的转换

由于不同的数据库的字段类型存在一定的差异，类型的名称不尽相同。在进行异构数据库间的数据移植前，必须定义好相关的字段类型的转换规则。根据 Oracle 与 SQL Server 的相关技术资料，总结了数据类型的转换对照规则，例如 SQL Server 中的 int、smallint、tinyint、bigint、bit、real、float、decimal 等数值类型均对应于 Oracle 中的 number 类型；SQL Server 中的 image 对应于

Oracle 中的 Blob 类型等。

5 数据移植的实现

5.1 数据导出

以 Access 为中间库的数据导出过程主要包含三个步骤：① 数据库环境准备，包括访问源数据库、清洗中间数据库；② 导出库表定义信息。③ 导出库表数据。下面结合工程实践给出具体的导出流程，如图 3 所示。其中检查主从表关系是指检查存在外键关系的主从表。需要注意的是由于不同数据库的保留字有所不同，所以从 Oracle 或 SQL Server 导出数据给 Access 时需要把原来的库表名称转换成内部自动生成的表名，并把对照关系保存在 USER\_TABLES 系统表中。由于导出时已经把库表的定义和数据分离，所以在 Access 中保存库表数据的数据表可以不考虑约束，并可以用统一的数据类型定义各个字段。

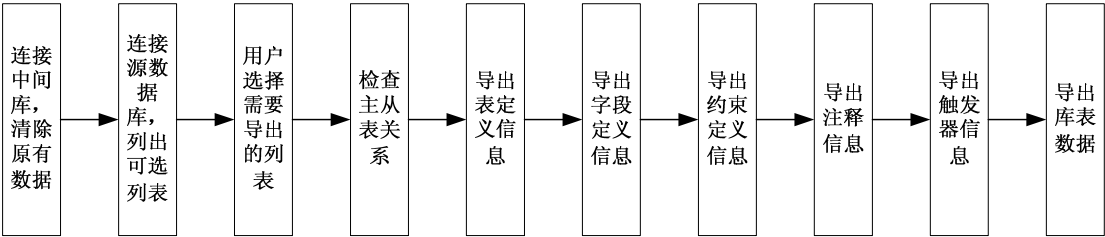


图 3 数据导出流程

5.2 数据导入

以 Access 为中间库的数据导入过程也主要包含三个步骤：① 数据库环境准备，包括访问目的数据库、中间数据库。② 库表结构的创建或校验。③ 导入库表数据。下面结合工程实践给出具体的导入流程，如图 4 所示。其中检查主从表关系

是指检查存在外键关系的主从表。由于在数据导出的时候已经保证了外键关系的主从表数据一致，所以在导入数据前可以先暂时关闭外键约束，待数据导入完毕后重启。这样处理，即使存在同一库表的不同字段之间存在外键关系的情况也能够顺利导入数据。

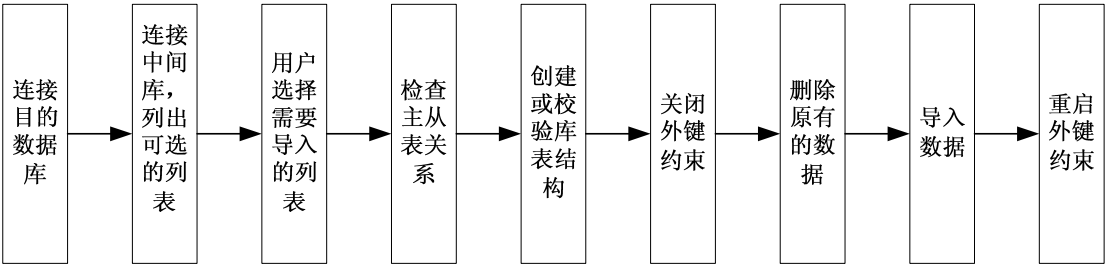


图 4 数据导入流程

## 6 结束语

异构数据库之间的数据移植是企业信息化建设正面临的巨大挑战, 本文根据工程实践的经验设计

并实现了一种基于 Access 中间库、库表数据和定义分离的数据移植方案。通过工程使用的情况表明, 该设计方案具有简单灵活, 应用范围广等优点, 为异构数据库的移植提供了一条新思路。

### 参考文献

- [1] 求是科技.SQL Server2000 数据库管理与开发技术大全[M] 北京: 人民邮电出版社, 2004.378-414.
- [2] 滕永昌.Oracle9i 数据库管理员使用大全[M] 北京: 清华大学出版社, 2004.607-618
- [3] 余琳, 陶欢, 高春颖.基于 XML 的异构数据库信息集成技术研究[J].现代军事通信, 2006, 14 (2) :48-51
- [4] 章小莉, 宁欣, 汪永好.SQL 完全手册 (第二版) [M]. 北京: 电子工业出版社, 2003.312-328

### 作者联系方式

通信地址: 南京市后标营 18 号总参第六十三研究所

邮政编码: 210007

联系电话: 025-80827332 13851811689

# 野战防空作战中的信息源校准技术

李芳芳 李新

**摘 要：**在野战防空作战中，防空导弹武器火力单元由于其定位定向装置的精度等问题，形成了信息源间的系统误差，系统误差的存在虽然不会对火力单元本身的作战造成影响，但对作战单元级指控系统的数据融合、空情通报、目标指示均有较大影响。本文介绍了系统误差形成的原因，提出了对信息源进行校准的方法，以及靶试试验中的验证结果。

**关键词：**野战防空；系统误差；信息源校准；地物；校飞；空情

## 1 简介

在野战防空作战中，各作战火力单元由于其定位定向装置的精度问题、寻北不一致等问题，造成了火力单元间的系统误差。由于火力单元所属的搜索雷达、跟踪制导雷达、发控、光电等分系统高度集成且存在严格的轴系关系，定位定向误差的存在不会对火力单元本身的作战造成太大的影响，但对作战单元级指控系统而言，需要将各火力单元的航迹信息进行同一性识别和融合，形成统一的信息场，各火力单元位置信息的不准确，将对数据融合功能有较大影响。此外，作战单元指控系统进行目标指示的目标以及向火力单元通报的目标都要转换到火力单元的坐标系中，位置信息同样具有较大的影响。本文在详细分析系统误差形成原因的基础上，提出了对信息源进行校准的方式和校准模型，

并给出了在靶试试验中的验证结果。

## 2 系统误差形成原因

假定两个信息源观测空中同一个目标，并将观测信息转换到同一坐标系，即使是在同一时刻转换，其结果也是不可能绝对一致的。它们之间的观测偏差是由以下原因引起的。

随机误差、系统偏差、换算系数的误差、或单个信息源定位定向信息的中断（紊乱）。出现系统误差的物理原因是：信息源大地连测不精确、水平轴对北不正确、传感器自身的系统误差、信息源距离比例有失真，这些因素均影响到在进行各种换算时信息源所使用的坐标系中，使得与目标实际的位置不一致。下面本文将分析雷达信息源不一致的坐标信息的详细形成机制。如图 1 所示。

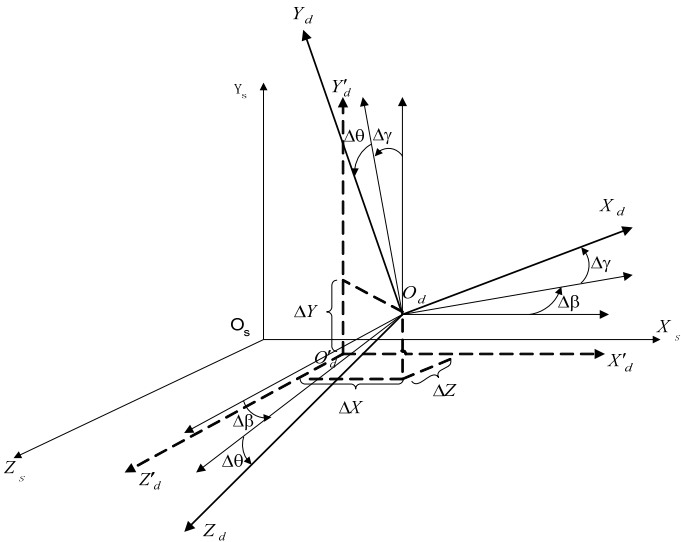


图 1 定向和大地连测误差

我们分析空间情况(图1),假定有两个信息源( $O_s$ 和 $O_d$ )在自己的坐标系中( $O_sX_sY_sZ_s$ 和 $O_dX_dY_dZ_d$ )测量,确定某一个点A的位置(图)。但是第二个信息源 $O_d$ ,在 $O_dX_dY_dZ_d$ 确定点A的坐标时,使用坐标系 $O'_dX'_dY'_dZ'_d$ 来计算,因此来自两个信息源的坐标信息不一致,为了使雷达信息一致,必须利用考虑了大地连测误差和定向

误差的校准。由图可知坐标系 $O_dX_dY_dZ_d$ 可以看做是坐标系统 $O'_dX'_dY'_dZ'_d$ 偏移了一个矢量 $(\Delta X, \Delta Y, \Delta Z)$ ,并且绕 $Oy$ 旋转了 $\Delta\beta$ ,绕 $Oz$ 旋转了 $\Delta\gamma$ ,绕 $Ox$ 旋转了 $\Delta\theta$ ,因此在坐标系 $O'_dX'_dY'_dZ'_d$ ,点的坐标按下式计算:

$$\begin{bmatrix} X'_d \\ Y'_d \\ Z'_d \end{bmatrix} = A \cdot \begin{bmatrix} X_d \\ Y_d \\ Z_d \end{bmatrix} + \begin{bmatrix} \Delta X \\ \Delta Y \\ \Delta Z \end{bmatrix}$$

$$A = \begin{bmatrix} \cos(\Delta\beta) \cdot \cos(\Delta\gamma) & -\sin(\Delta\gamma) & \sin(\Delta\beta) \cdot \cos(\Delta\gamma) \\ \cos(\Delta\beta) \cdot \sin(\Delta\gamma) \cdot \cos(\Delta\theta) + \sin(\Delta\beta) \cdot \sin(\Delta\theta) & \cos(\Delta\gamma) \cdot \cos(\Delta\theta) & \sin(\Delta\beta) \cdot \sin(\Delta\gamma) \cdot \cos(\Delta\theta) - \cos(\Delta\beta) \cdot \sin(\Delta\theta) \\ \cos(\Delta\beta) \cdot \sin(\Delta\gamma) \cdot \sin(\Delta\theta) - \sin(\Delta\beta) \cdot \cos(\Delta\theta) & \cos(\Delta\gamma) \cdot \sin(\Delta\theta) & \sin(\Delta\beta) \cdot \sin(\Delta\gamma) \cdot \sin(\Delta\theta) + \cos(\Delta\beta) \cdot \cos(\Delta\theta) \end{bmatrix}$$

在已知某些点(在坐标系 $O'_dX'_dY'_dZ'_d$ 和 $O_dX_dY_dZ_d$ 的坐标系)的条件下就能够进行必要的校准。

在图2提供了两个信息源观测A目标的情况。假定对于两个信息源来说,系统的大地连测误

差都存在,对于标准信息源为: $\Delta X_{ps}$ ,  $\Delta Y_{ps}$ ,  $\Delta Z_{ps}$ ,对于被校准信息源为 $\Delta X_{pd}$ ,  $\Delta Y_{pd}$ ,  $\Delta Z_{pd}$ ,系统的定向误差( $\Delta\beta$ ,  $\Delta\gamma$ ,  $\Delta\theta$ )和比例畸变系数,只对被校准的信息源才有。

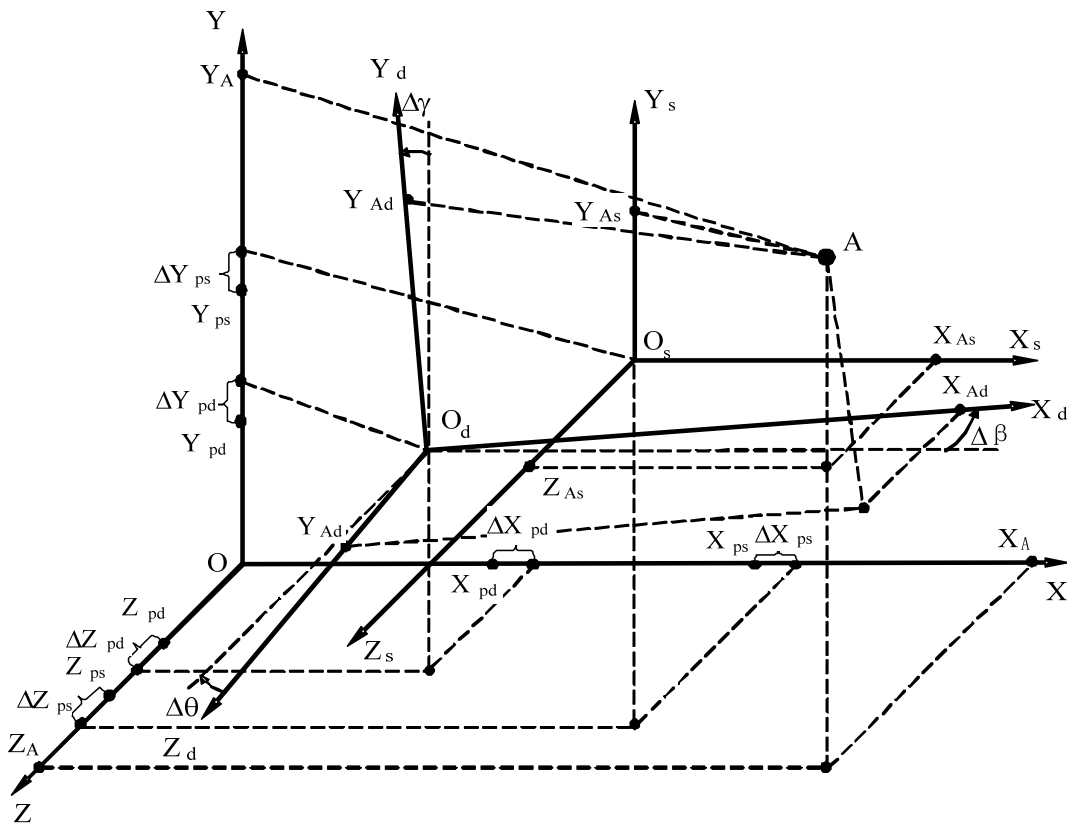


图2 在两个信息源坐标系中A的位置

在图中, 采用了以下的符号。

$OXYZ$  ——作战单元指控系统的约定点坐标系 (简称约定点坐标系);

$O_s X_s Y_s Z_s$  ——标准信息源的坐标系统;

$(X_{ps}, Y_{ps}, Z_{ps})$  ——在约定点坐标系中, 标准信息源的位置;

$O_d X_d Y_d Z_d$  ——被校准信息源的坐标系统;

$(X_{pd}, Y_{pd}, Z_{pd})$  ——在约定点坐标系中, 被校准信息源的位置;

$(X_A, Y_A, Z_A)$  ——在约定点坐标系中, 点 A 的坐标;

$(X_{As}, Y_{As}, Z_{As})$  ——在标准信息源中, 点 A 的坐标;

$(X_{Ad}, Y_{Ad}, Z_{Ad})$  ——在被校准的信息源坐标系中点 A 的坐标;

$\Delta X_{ps}, \Delta Y_{ps}, \Delta Z_{ps}$  ——标准信息源的大地连测

误差;

$\Delta X_{pd}, \Delta Y_{pd}, \Delta Z_{pd}$  ——被校准信息源的大地连

测误差;

$\Delta\beta, \Delta\gamma, \Delta\theta$  ——定向系统误差。

### 3 信息源校准

#### 3.1 校准方法

由于系统误差的存在, 对于同一个目标, 在作战单元显控台上可看到不同的目标, 如图 3 所示, 对于目标 P、T、S, 在平面上可到  $P_1$ 、 $P_2$ 、 $T_1$ 、 $T_2$ 、 $S_1$ 、 $S_2$  六个目标。

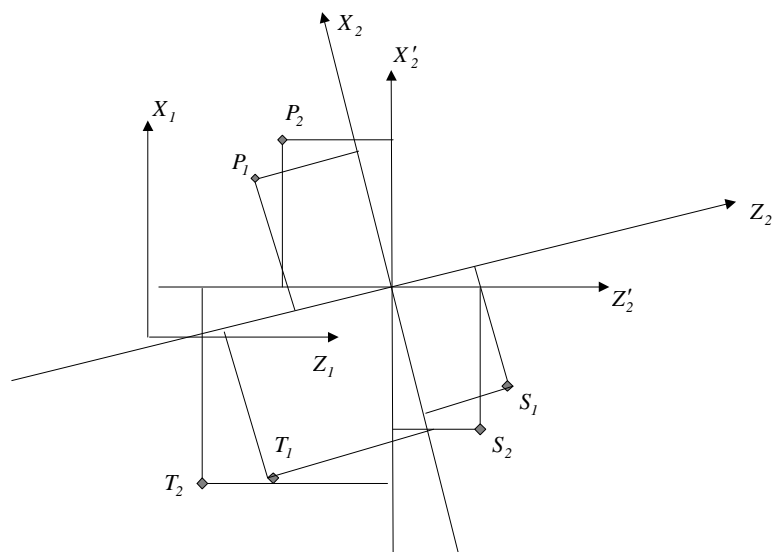


图3 在平面上定向的情况

当两个信息源上报的关于相同目标的信息足够多时, 就可利用上报的信息进行信息源的校准, 且较少地受到随机测量误差的影响。

以两个雷达站  $I_1$ 、 $I_2$  为例, 站  $I_1$  约定为标准站, 相对于它来对站  $I_2$  进行校准。校准是在站  $I_1$ 、 $I_2$  测量到的一个对象的直角坐标的统计数据基础上进行的, 这个对象处于运动中。

假定  $X_1 = (x_1 \ y_1 \ z_1)^T \in \mathbf{R}^3$  是在站  $I_1$  所测量的被观测对象的直角坐标的列矢量, 并折算到站  $I_2$  坐标系中,  $X_2 = (x_2 \ y_2 \ z_2)^T \in \mathbf{R}^3$  是由站  $I_2$  所测量的同一个对象的坐标的列矢量。假定  $\delta > 0$  ——未

知的距离比例的畸变系数;  $A = (a_{jk})$ ,  $(j, k = 1, 2, 3) - (3 \times 3)$  ——站  $I_2$  相对与  $I_1$  定向误差所形成的未知系数矩阵;  $\Delta = (\Delta X \ \Delta Y \ \Delta Z)^T \in \mathbf{R}^3$  ——大地连测未知误差的列矢量; 信息源坐标测量是带有随机误差  $\xi_i = (\xi_{i1} \ \xi_{i2} \ \xi_{i3})^T \in \mathbf{R}^3$ ,  $(i = 1, 2)$ 。假定误差的随机矢量  $\xi_1, \xi_2 \in \mathbf{R}^3$ , 是未知的且具有带有零方差的三维的高斯分布。

$$L\{\xi_i\} = N_3(0, \Sigma_i) \quad (1)$$

其中  $\Sigma_i = (\sigma_{ijk}) - (3 \times 3)$  是随机误差协方差矩阵。

因此,假定在数学统计中一般用高斯观测模型。

$$X_i = X_i^0 + \xi_i, \quad i=1,2 \quad (2)$$

其中  $X_i^0 = (x_i^0 \ y_i^0 \ z_i^0)^T \in \mathbf{R}^3$ ——如果没有测量的随机误差,是由站  $S_i$  测量的对象的直角坐标的真实值的列矢量。

根据距离比例畸变的已知的物理特性  $\delta$ , 定向误差  $A$  和大地连测误差  $\Delta$  可用以下的矩阵模型来进行校准:

$$X_1^0 = \delta \cdot A \cdot X_2^0 + \Delta \quad (3)$$

因为参数  $\delta, A, \Delta$  是未知的,要在公式 3 计算它们时,我们推断  $3 \times 3$  的矩阵  $A' = \delta \cdot A$  和  $3 \times 1$  列矢量  $\Delta$  就是被识别的未知的参数。

利用站  $I_1$ 、 $I_2$  上报目标的统计数据,利用多元线性回归和向量的极大似然估计来进行参数的解算。

### 3.2 校准方法的应用

在工程中应用时,信息源校准的方式主要有三种:根据地物的校准、根据校飞目标的手动校准以及根据空情的自动校准。

根据地物的校准是指定一个地物,由信息源对指定的地物进行观测,作战单元接收到各信息源上报的地物信息后进行校准,该方法的精度较高,但对信息源以及环境的要求较高。

根据校飞目标的校准是指在校飞状态下,信息

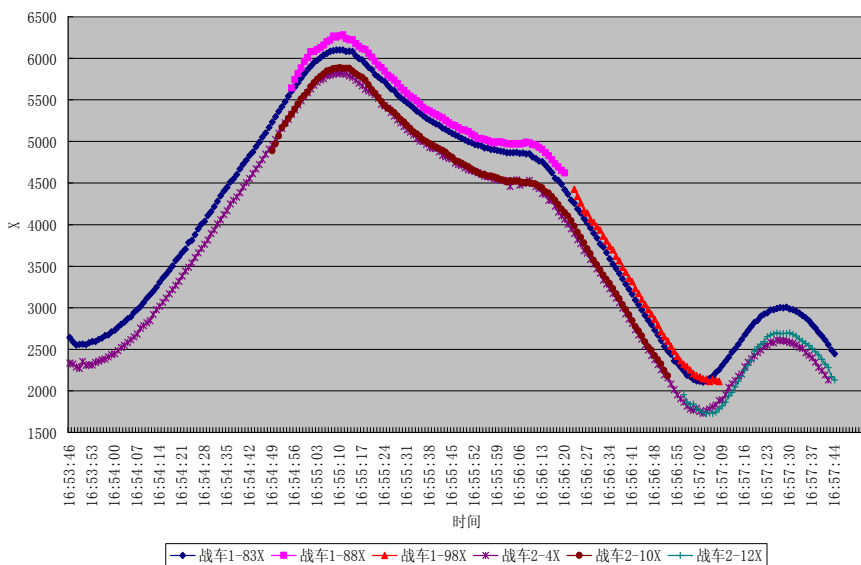
源将观测的校飞目标测量值上报给作战单元,作战单元的操作员人工划定同一个目标的区域,处于该区域内的目标认为是同一个目标,根据上报的目标数据进行校准。此种方式下,由于校飞目标少,减少了由于同一性识别错误造成的对校准的影响,精度也比较高,但要求进行校飞试验。

根据空情的自动校准是指在作战状态下,根据各信息源上报的空情信息自动进行校准计算,不需要人工参与。

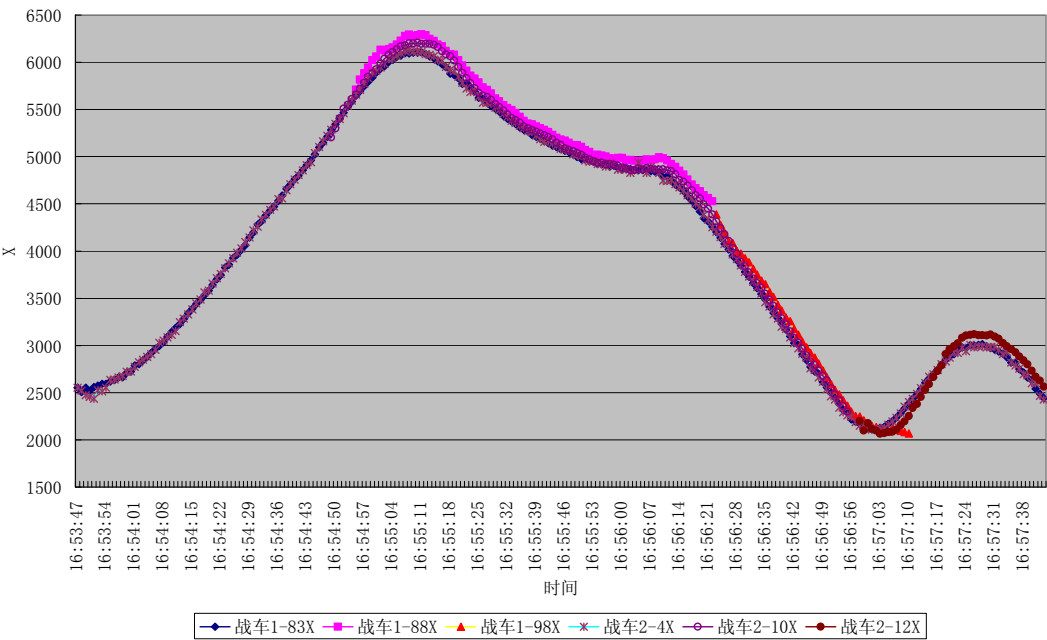
校准计算能够给出当前的校准系数,当操作员观察到当前各信息源间相互的校准系数以及信息源综合校准系数较高时,可启动校准补偿。在启动校准补偿后,作战单元接收到各信息源的局部航迹时,将对航迹进行补偿,在向信息源进行目标指示、通报目标时同样需要利用校准参数进行目标航迹信息补偿。

## 4 试验验证

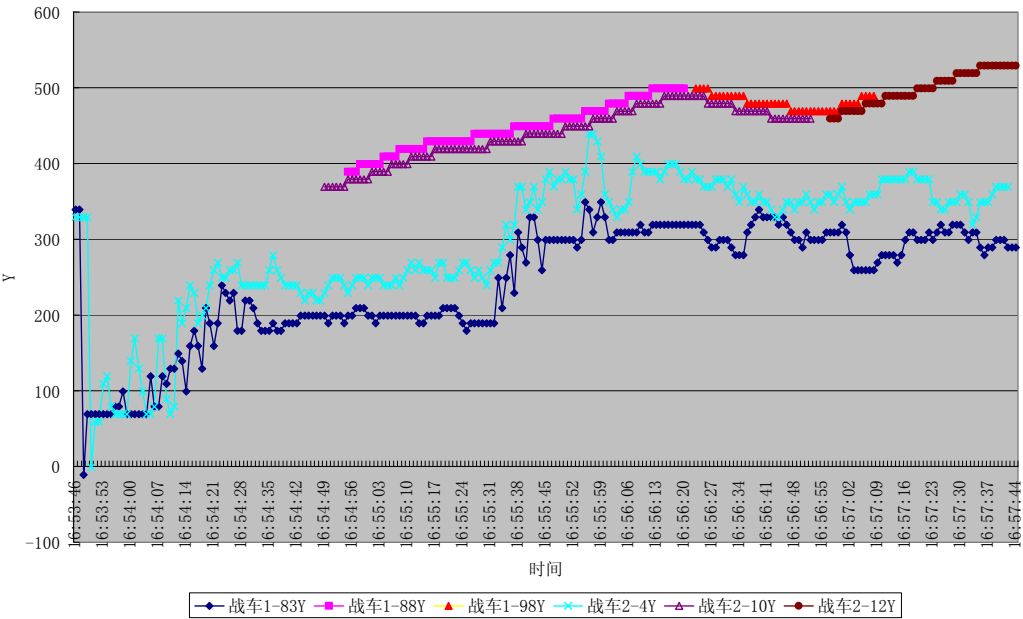
在某野战防空导弹武器的飞行试验中,作战单元采用了校准功能,对信息源的系统误差进行补偿。试验中采用了利用空情的自动校准,某次飞行试验的结果见图。其中战车 1、战车 2 分别为两个火力单元。



(a) 信息源输入航迹—X 轴

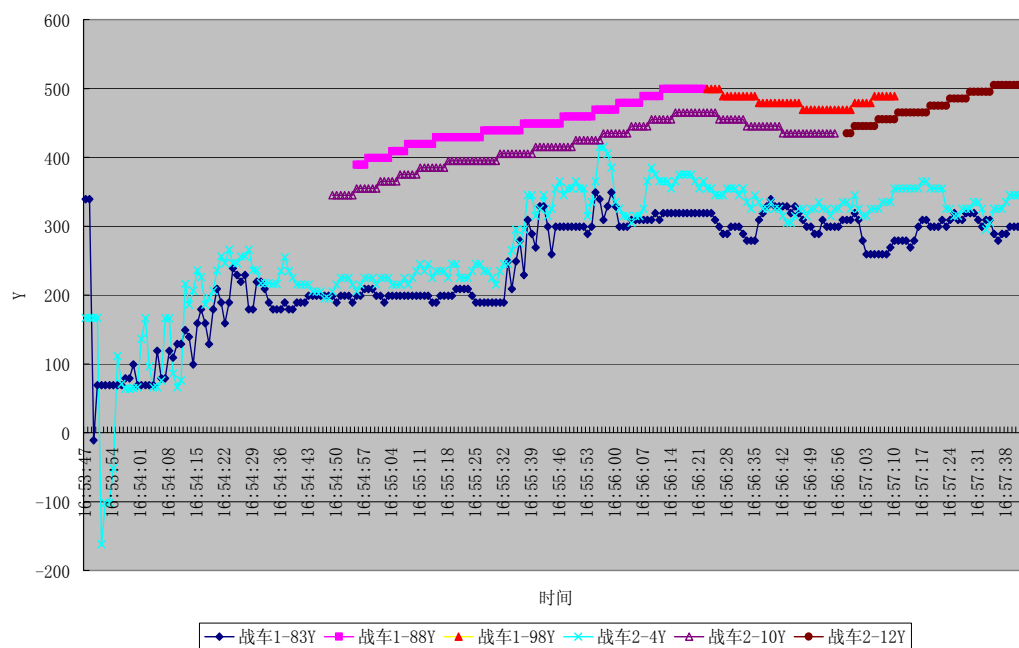


(b) 补偿后的信息源航迹—X 轴

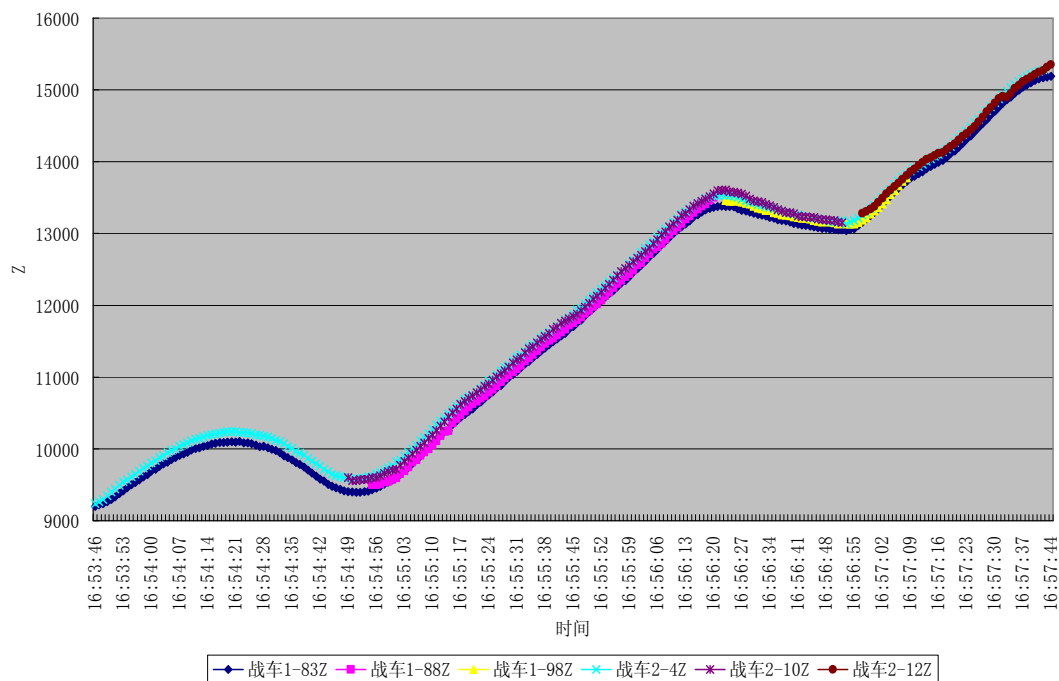


(c) 信息源输入航迹—Y 轴

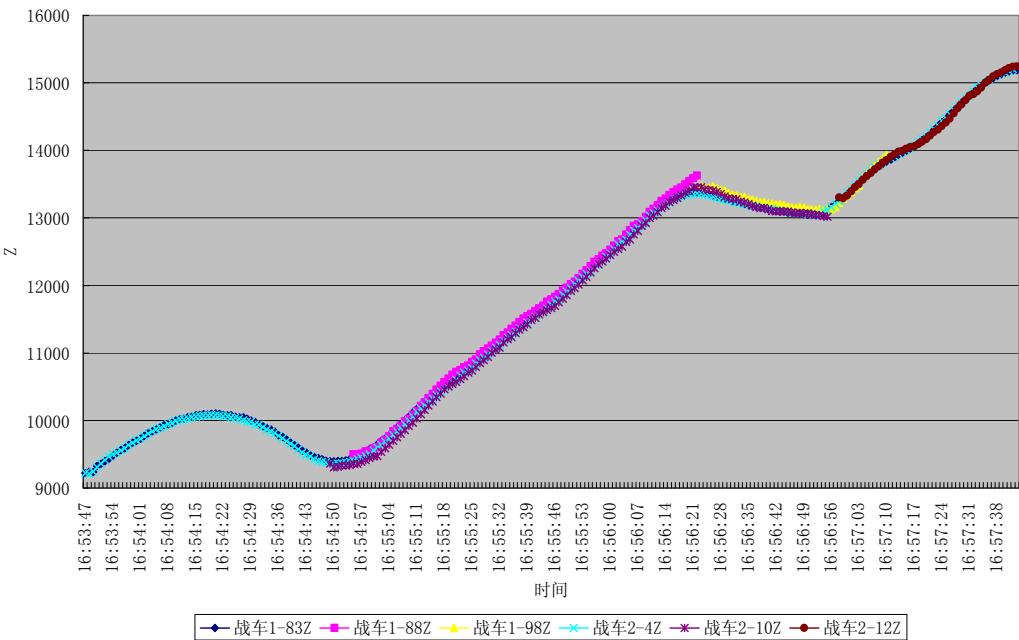




(d) 补偿后的信息源航迹—Y轴



(e) 信息源输入航迹—Z轴



(f) 补偿后的信息源航迹—Z 轴

图 4 信息源输入航迹与补偿后的信息源航迹

表 1 信息源输入航迹与补偿后的航迹比较

	输入 X 差 值平均值	补偿后 X 差 值平均值	输入 Y 差 值平均值	补偿后 Y 差 值平均值	输入 Z 差 值平均值	补偿后 Z 差 值平均值	备注
战车 1-83 与战车 2-4	325.9	17.3	56.6	37.4	148.2	25.3	航迹关联
战车 1-88 与战车 2-10	406	78.0	13.7	37.5	112	113	航迹关联
战车 1-98 与战车 2-10	441.6	70.8	13	36.7	58.6	76.3	战车 1-88 消失 后关联
战车 1-98 与战车 2-12	391.4	54.6	10.8	34	63.9	35.6	战车 2-10 消失 后关联

从图 4 和表 1 中可以看出，校准功能均能够有效地消除不同信息源之间的定位和定向误差。

5 小结

本文在分析系统误差形成原因的基础上，介绍

了信息源校准的方法以及在工程中的应用方法，给出了在某野战防空导弹武器系统试验中的验证结果。经仿真环境以及实际装备飞行试验的验证，校准功能能够有效地消除系统误差。

参考文献（略）

作者联系方式

通信地址：北京市 142 信箱 15 分箱  
邮政编码：100854  
联系电话：13366063732 （张煜冲）

# 舰船装备技术保障信息系统初探

李峰 曹原

**摘 要：**舰船装备技术保障信息系统以提高舰船装备技术保障的快速反应能力和指挥自动化水平为宗旨，基本满足战时技术保障指挥决策和平时业务管理需要，实现与作战指挥信息系统的互联互通。并可根据战时需要和首长指示，快速、合理地拟制多种可供首长决策参考的装备保障计划方案，快速传递动员指令和有关信息，提高现代局部战争条件下舰船装备技术保障的速度和质量。

**关键词：**舰船装备；技术保障；信息系统

由于高技术条件下的现代战争具有突发性、紧迫性、危急性等特点，致使预先制定的装备保障计划难以完全满足战争的要求，为了及时做出新的装备保障决策，需要建立能适应战争情况变化的智能化装备保障系统。当前，信息获知与处理能力、决策与应变能力是装备保障快速反应能力的决定性因素，装备信息获知的多与少、实与虚，对于装备保障的规模、数量、形式、方法、程序都有着十分重要的影响。为此，探索开发海军的舰船装备技术保障信息系统，其目的就是收集、处理各方面装备的信息，科学、有效地对海军舰船进行装备技术保障，提高装备技术保障的效率，保证海军舰艇的完好率，实现装备技术保障的办公自动化，为首长决策提供依据。

## 1 舰船装备技术保障信息系统标准

### 1.1 系统体系结构规范

海军舰船装备技术保障信息系统涉及多部门、多层次，由若干子系统相互连接和相互作用，要求协调一致的系統，其建设周期长、投入大，因此需要在建设过程中，在各种不同的层次上规划系统的体系结构特征，并将其规范化，形成体系结构框架，指导系统建设和发展。此外，在确定体系结构规范时，必须考虑如何对信息化建设中所包含的单位和部门，准确描述其职能，对其所要完成的任务、活动、维护和使用的信息进行明确的设计和定义。

目前来看，可以借鉴美军的做法，从“任务、系统、技术”三个不同的视点来描述海军舰船装备

技术保障信息化建设及其组成系统的体系结构。其中：任务视图描述了海军装备技术保障信息化需要完成的任务和行动、以及要求的信息流。系统视图描述为装备技术保障提供信息的系统及其互联关系。技术视图提供一组技术标准、规则和惯例，用来实现特定信息系统的服务、接口和互联。

### 1.2 系统技术标准与规范

由于信息技术具有开放性和军民两用的特点，并且许多相关技术已在工业中成熟的应用。因此，海军装备技术保障综合信息系统的技术标准与规范可以建立在民用技术乃至国际市场的基础上，强调较为通用的商业和政府标准，在选择舰船装备技术保障信息系统的技术标准与规范时可考虑如下原则。

- 1) 互操作性：增强和支持联合能力和潜在的信息变换能力；
- 2) 成熟性：技术上成熟和稳定，在市场上有强大的技术支持；
- 3) 可实现性：技术上可行，在实现上不受专利约束；
- 4) 公开使用的标准优先考虑；
- 5) 与法律规章、政策和指导方针无冲突；
- 6) 优先采用军队、国内或国际工业标准。

## 2 舰船装备技术保障信息系统结构

### 2.1 系统总体结构

舰船装备技术保障信息系统以数据库为基础，以信息网络为载体，以数据中心为枢纽，通过信息

采集、分析和评估等手段，以舰船装备技术保障信息为数据源，以统一的信息化标准、相关政策法规与管理制度、专业化、信息化管理为保障，形成以舰船装备技术保障、统计分析信息发布、信息查询及决策支持等为核心的一体化的舰船装备技术保障信息系统，如图 1。舰船装备技术保障信息系统包括技术支持系统、信息交流系统、规章制度系统、组织结构系统、规划计划系统、文书管理系统、设

备管理系统、财务管理系统、信息发布系统和后台管理信息系统等 10 个子系统的综合信息处理平台，基本上涵盖了舰船装备技术保障中的所有业务。系统根据相应的条令条例和规章制度，将 GIS（地理信息系统）集成于办公办文系统之中，实现图文一体化管理，达到舰船装备技术保障计算机化，提高舰船装备技术保障的水平、效率和质量，促进舰船装备技术保障的科学化。

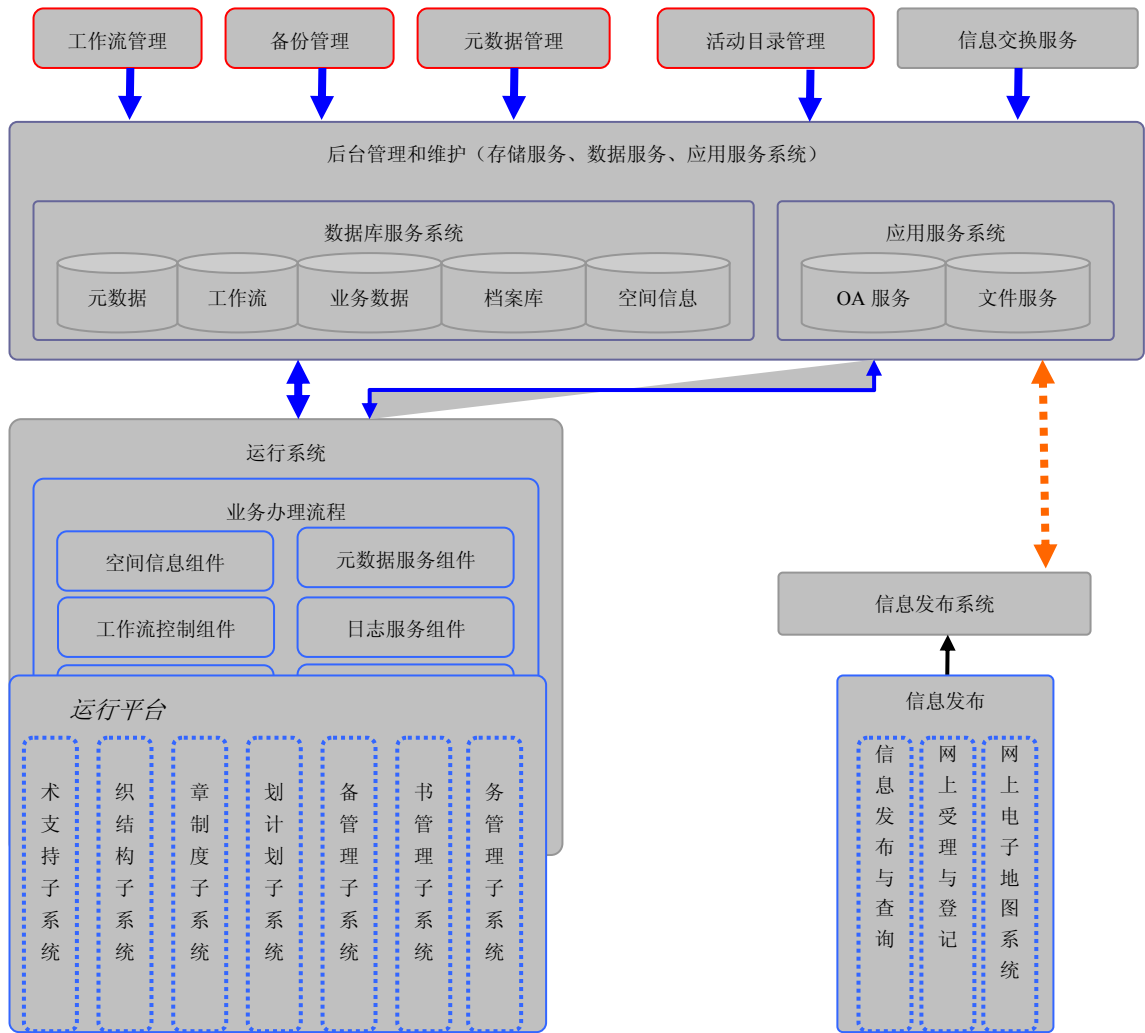


图 1 舰船装备技术保障信息系统结构图

2.2 系统运行模式

系统采用海军级、基地级、舰员级系统运行模式，构成完全网络化的运行环境。海军级和基地级系统分别在各自的软硬件环境和数据库支持下运行，舰员级系统作为基地级系统的远程工作终端以及独立的单机软件系统运行。

- 各级之间可以自行管理和维护，同时在数

- 据规范、编码标准、交换格式、系统接口、技术规范等方面进行统筹规划；
- 统一的数据规范和编码标准，方便实现数据交换和共享；
  - 软件及其开发工具支持数据库技术；
  - 各级系统具备共同的数据交换接口定义、软件工具和交换方法；

2.3 数据管理模式

整个系统的数据库分布于海军和基地二级数据中心。数据中心由数据库、数据库管理系统和相应的网络系统、业务系统等组成，为本级各类应用系统的运行提供数据支持和软硬件环境支持。数据库管理采用集散式数据存储模式，即海军级系统集中保存所有相关数据，基地级系统存储各自的数据库，通过网络（或光盘等其他介质）定期（或实时）复制（或备份）数据到上级数据中心。海军级、基地级数据库各自独立维护、存储。基地级系统的数据主要有两种形式向海军级汇集，一是实体数据（即系统运行中的各项具体数据），二是统计数据（即用于统计汇总上报的数据），海军级系统均保留该两种数据的备份。

在舰船装备技术保障过程中，各级系统使用本地局域网数据，从而避免跨网实时调用数据带来的不稳定性和低效率、高成本的缺点；数据交换应通过专用的工具模块和数据服务模块进行，原则上不允许直接访问不同级别的数据库；数据共享服务通过海军级统一进行协调，从而保证数据的唯一性、一致性和权威性。这种方式既能进行集中化的管

理，方便数据的使用和备份，保证数据的安全性，同时又能获得分布式数据库的各项优点，这是与舰船装备技术保障信息数据量大、更新周期长、多级分布式管理的特点相适应。

2.4 系统网络结构

目前舰船装备技术保障工作具有分级式管理、分布式存储、网络化运行的特点。适应该特点的要求，系统的网络逻辑拓扑应该采用“异地互备集群结构”，从而为上述的系统运行模式和数据存储模式提供支撑。海军机关可以采用异地的两个机房和相应的服务器系统构成异地互备系统，异地之间通过专网进行服务器间的数据同步，在正常情况下，两地局域网的数据库服务器同时运行，当其中一台服务器发生故障时，可以使用另外一台服务器继续工作；海军与各基地之间通过专网同时也构成异地互备系统，数据库在海军、基地之间同时保存，通过定期或实时复制的方式进行同步，有条件的基地也可以在基地实现双机备份系统从而进一步提高系统的可靠性。其逻辑结构如图 2 所示（实线表示局域网连接，虚线表示专网或 VPN 连接）。

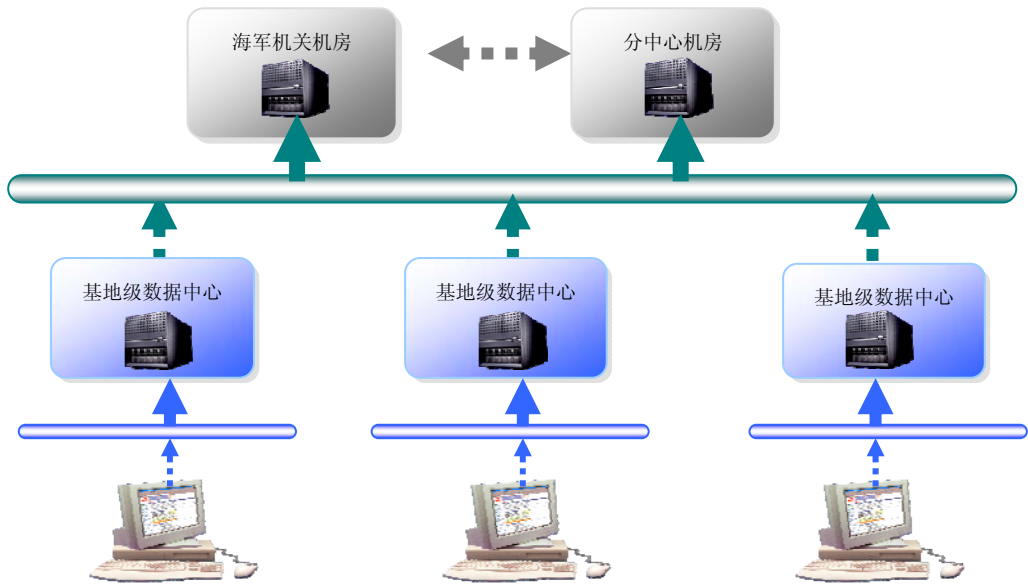


图 2 异地互备网络配置总体拓扑结构示意图

该结构具有以下特点。

- 异地容灾：当一地发生灾难性事故时，另一地系统仍然能够保持运行，数据不会遭受毁灭性损失；
- 高性能：实现了双机无冗余备份，处理能

力被充分利用，有利于提高系统性能；另外，大数据量的空间信息访问使用本地存储，更加快了运行速度；

- 低带宽：由于采用服务器间数据同步，避免网络流量在广域连接关键路由上的汇

集，有效降低了跨子网访问的带宽需求；

- 低成本：该结构在目前的网络条件下能够实现，软、硬件成本低，维护简单，运行成本较低。

该结构相对于集中化的“双机集群模式”而言，是一种松散型集群结构，不仅有利于提高系统稳定性和安全性，而且可以大幅度提高系统的性能。

2.5 系统模块结构

舰船装备技术保障信息系统的结构与功能从总体结构和功能分配方面统一考虑，系统的数据库及软件模块可以在其他子系统中重用，以减少今后系统开发和维护的工作量。

按照功能构成，软件系统可分为四个主要部

分：系统管理和维护系统、运行平台、GIS 图形应用模块、信息发布系统，其结构如图 3 所示。系统管理和系统维护主要是对系统工作流程、机构、服务参数等信息流进行调控，按照业务流程和规则，实现信息的路由，并对工作过程和进度进行控制，控制 GIS 的应用和办公自动化组件的调用及信息传输。运行平台即办公办文系统，为工作人员日常办公提供各种信息处理工具，主要是文档、表格的录入、修改、查询检索、统计分析、输出（屏幕显示、打印输出）等。GIS 图形应用模块，主要提供业务办理过程中所需的空间数据录入、修改、查询检索、统计分析、制图等功能。信息发布系统是将部队装备技术保障有关的信息通过终端向使用者发布，系统所发布的信息包括空间信息和非空间信息。

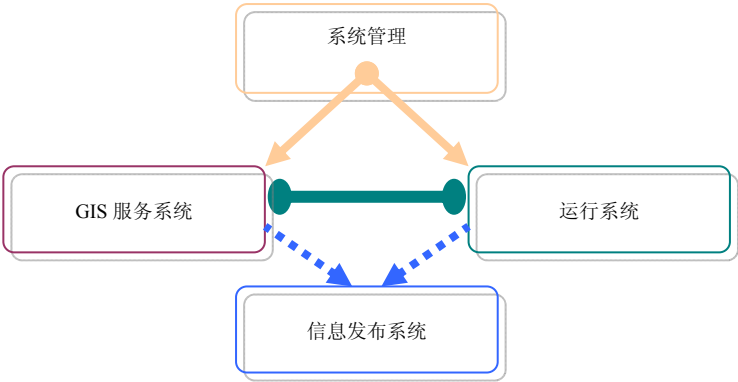


图 3 系统模块结构示意图

2.6 系统安全体系

安全是系统正常运行的保证。舰船装备技术保障信息系统应建立一个合理、实用、先进、可靠、综合统一的安全保障体系，确保信息安全。采用身份认证、密码凭据保护、IP 地址访问控制、入侵检测、容错容灾、数据安全交换、系统日志管理等技术。

3 舰船装备技术保障信息系统功能

3.1 装备保障数据库

装备保障数据库以各类舰船装备的统计数据为基础，按需要存储管理各类数据，提供网络、软盘、键盘等多种输入方式，方便快速地录入数据。数据库的结构易于扩充和修改，可以通过条件方式

迅速、准确地对所需数据进行条件和模糊查询，并对结果进行统计和比较。数据库可在本级和多级联网运行。

3.2 装备保障实力统计

由基地装备部牵头，会同作战、军务、干部等部门做好保障机构、专业人员实力统计，准确掌握装备保障力量及分布情况。当某型装备发生故障时，基地机关将装备型号输入后，计算机即可查找有关的备品存储情况，并根据装备分类自动提供能够维修该装备的专业技术人员名单。

3.3 信息浏览查询

可输入关键词进行自动查询。装备维修保障后，其工作时间、维修配件、存储数量等将发生变化，需根据反馈信息由机关人员进行更新。只要数

数据库平时维护及时，查询的数据就准确无误。所有查询结果，都可以用图表和卡片的形式打印出来。

### 3.4 装备保障计划辅助决策

舰船装备技术保障信息系统，能根据首长和上级的指示，通过条件选择方式，自动拟制多种可提供首长参考的装备保障计划方案，重点解决装备按专业对口筹措、保障的需要，以提高装备保障的速度和质量，提高战时舰船的作战能力和生命力。为了保证系统的正常运行，该系统还设置了系统维护模块，主要是完成日常数据备份、恢复，逐级上报磁盘等功能。

## 4 舰船装备技术保障信息系统作用

### 4.1 提高装备保障的快速反应能力

在对原始数据信息进行了正确归纳演绎和逻辑分析后，将使下一次维修保障变得有历史可查、有情况可预见，为下一次维修保障提供了重要信息，加大了故障判断的准确性和故障排除力度。通过对以往故障的统计和分析，可以给年轻的维修人员提供极有价值的参考信息，无异于一个有丰富经验的专家指导，从而迅速地得到大体的故障范围及解决办法。对于有经验的专家也能提供有参考意义的信息。另外，将每次成功维修后信息数据再添加进数据库，又为以后的统计分析提供了宝贵信息，进而达到了良性循环，使得以后的归纳演绎和逻辑分析结论更加接近实际，更有帮助价值，加强了装备保障力量。

### 4.2 合理配置备件数量

通过对发生故障的准确统计和正确分析，可以

了解装备在不同情况下（如训练强度、外界温度等）的常见故障和易损坏部件情况。我们可以对备件的数量进行调整，对于磨损严重或出现故障频繁的备件多配备一些，而对于不常发生故障的备件少配备一些，使得备件的数量和结构更趋合理、更加优化、更具科学性，从而提高保障效率，减少置而不用、浪费资源的现象。与此同时，备件的经费开支也将相应减少。

### 4.3 反馈装备生产厂商

通过对服役装备故障进行统计分析，可以得到装备中哪些部件因为使用环境的变异而易于发生哪些故障，哪些性能需要提高。将此信息反馈给装备生产厂商，他们通过对这些部件的生产原材料、制造工艺等进行改进提高，从而设计生产出整机性能更好的装备。另外，面对我军装备型号多且杂的现象，对不同型号的同类装备可以进行比较得到哪种装备最实用，我们可以根据此信息来选购最好的装备。

### 4.4 加强人员管理

舰船装备技术保障中的人员管理将故障类型与修理专家挂钩，通过现代通信网络手段实现千里之外处理故障。在应急机动装备保障分队构建时，其人员主要来自于我军自身的维修保障力量，这些针对特定装备的一线维修保障人员名单的统计，可以使决策者在突发事件需要建立应急机动保障分队时，有最适合的组成人员名单可供选择，提高了决策者的决策效率。

参考文献（略）

作者联系方式

通信地址：海军装备研究院综合所政策管理与外军室

邮政编码：100073

联系电话：010-66952494



# 基于HLA炮兵作战指挥视景仿真系统的设计与实现

李汉琛 李广文

**摘 要:** 现代战争对炮兵作战指挥的要求不断提高,传统的炮兵作战指挥训练手段已难以满足要求。随着分布交互仿真体系结构和虚拟仿真技术的发展,开发一套基于 HLA 的炮兵作战指挥仿真训练系统成为可能。本文介绍了炮兵作战指挥仿真训练系统的总体框架,规划了视景仿真系统的各项功能单元,详细说明了视景仿真系统的联邦设计,并且实现了 Vega 线程与仿真线程的通信。运行表明,该系统能够演示出仿真的全过程,并且满足系统仿真的实时性要求。

**关键词:** 分布交互仿真; 视景仿真; 炮兵作战

传统的炮兵作战指挥训练大多局限于室内想定作业和战术推演,手工作业成分较多,组织复杂,高技术含量低,效果差,难以满足现代战争对炮兵提出的实时、准确、快速、可靠和连续性要求,因而利用现代计算机仿真技术、网络技术开发炮兵作战指挥仿真训练系统,来进行训练是非常必要。

本文针对炮兵作战指挥仿真训练系统的视景需求,基于 MultiGen Creator 三维仿真建模软件和 Vega 视景仿真软件,通过基于 HLA 的视景联邦设计和解决多通道显示、坐标转换、视点方式选择、视景线程与仿真线程的数据同步等关键技术,设计并实现了炮兵作战指挥视景仿真系统。

## 1 炮兵作战指挥仿真训练系统简介

炮兵作战指挥仿真训练系统开发的主要目的是通过对具有互操作和可重用性的炮兵群联邦仿真成员的开发、集成、运行和管理工作,探索基于 HLA 技术规范分布式交互仿真应用系统的开发、管理与运行体制。系统具备的基本功能主要如下。

在训练内容上,能够满足炮兵部队(分队)指挥作业、战术演练、集团作业和战法研究的需要;在训练对象上,能够满足相应类型部队(分队)指挥员进行战术指挥训练的需要;在训练方式上,能够进行单机训练、本地或异地多机训练等。

炮兵作战指挥仿真训练系统主要包括红方联邦成员组、蓝方联邦成员组、控制方联邦成员组。红方联邦成员组包括:炮兵群指挥所、群观察所、炮兵营、炮兵连、营观察所、连观察所等作战单位。

蓝方联邦成员组包括:蓝方合成部队等。控制方联邦成员组包括:HLA/RTI 运行服务器、二维态势显示成员、三维视景成员、仿真联邦管理成员和仿真数据记录成员。这里的三维视景成员即为本文研究的基于 HLA 炮兵作战指挥视景仿真系统,用来为炮兵作战指挥仿真训练系统(联邦)提供三维视景支持。

## 2 炮兵作战指挥视景仿真系统的分析与设计

### 2.1 系统功能分析

炮兵作战指挥视景仿真系统主要是提供一个虚拟战场环境并实时显示系统仿真演练的结果。具体功能如下。

#### 2.1.1 建立一个逼真的虚拟战场环境

场景及其模型的逼真性是视景仿真的基本要求。视景仿真训练提供给参训人员的应该是一个尽可能接近真实场景的虚拟场景,在满足仿真视景渲染的基础上,尽量使用精细的模型,以达到逼真的效果。

#### 2.1.2 对所有作战实体仿真结果进行实时三维显示

实时性是视景仿真系统本系统的重要功能,也是本系统要解决的重点问题。视景仿真系统的实时性直接关系到指挥人员能否做出正确的决策,从而



影响作战指挥训练的效果。

2.1.3 典型局部战场的漫游

为指挥员提供战场漫游，便于指挥员更清楚地把握战场情况，但这种漫游，没必要面面俱到，只需将指挥员带到感兴趣“热点”区域，获得需要的信息即可。另外硬件上的限制，也无法满足将整个战场同时调入的需要。

2.1.4 视点切换与控制

为了满足不同仿真成员对视景的需要，系统应该具备在任意地点、以多种方式观察战场的功能，因此，应提供灵活的视点设置方式以及不同时点之间的切换方式。

2.2 系统功能模块划分

根据仿真工作流程，将视景联邦成员划分为以下几个功能模块：RTI 接口模块、视景生成模块、参数转换模块、人机交互模块和视景显示模块。在视景显示模块中将虚拟场景的视景环境控制、视景

仿真实体控制和观察者控制独立出来，充分保证了系统的扩展性，便于各自模块的独立测试<sup>[1]</sup>。其功能单元结构如图 1 所示。

视景生成模块独立于系统之外，其实质就是利用 Creator 三维建模软件建立地形模型和武器实体模块。RTI 接口模块用以完成创建联邦、加入联邦、制定时间策略、注册对象类、订购对象类、交互类等系统初始化工作；维护联邦执行，其间反射对抗视景仿真系统所订购的各对象类、交互类以及最后的退出和撤销联邦执行操作，并将这些交互信息发送到参数转换模块。参数转换模块接收来自人机交互模块的控制信息，该模块将这些外部信息转化成三维视景系统内部能够辨别的表现命令，并将这些表现命令发布。视景生成模块负责生成系统所需的视景数据库，包括地形数据，人文特征数据和实体三维造型。插件管理模块负责完成插件管理工作，包括插件的创建和销毁，允许用户能系统功能进行部分扩展。视景显示模块订购并接收到消息，根据参数进行处理，并生成仿真视景加以显示。

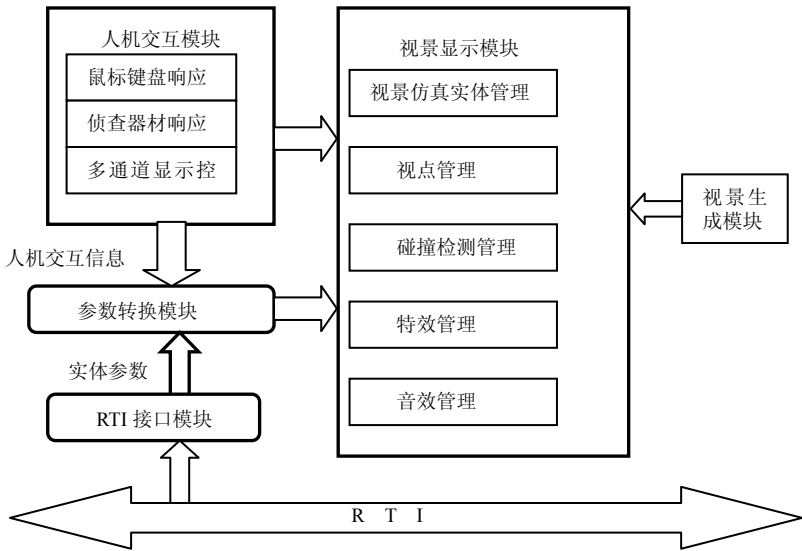


图 1 功能单元结构图

3 系统实现解决的几项关键技术

3.1 基于MultiGen Creator的三维视景建模

视景模型是对原型的模仿和描述。战场环境模型一般分为地形模型、气候环境模型、特殊环境模型、声音环境模型和动态实体模型五大类<sup>[2]</sup>，这里

只对地形建模和动态实体建模加以介绍。

3.1.1 地形建模

地形对炮兵部队的机动、侦察、火力发挥、毁伤、通信及电子对抗等影响极大，在指挥决策中，研究地形、利用地形、趋利避害，对有效正确实施炮兵作战指挥具有重要意义。因此，对地形仿真真是

进行炮兵作战指挥环境仿真首先要解决的问题。（图 2 所示）。

建造地形模型的一般过程可分为六个阶段（如

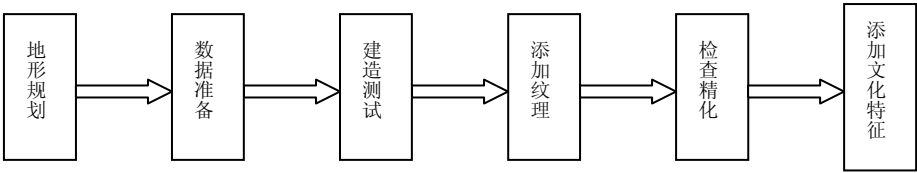


图 2 地形建模的一般过程

3.1.2 动态实体建模 步骤（如图 3）如下。

使用 MultiGen Creator 对动态实体建模的一般

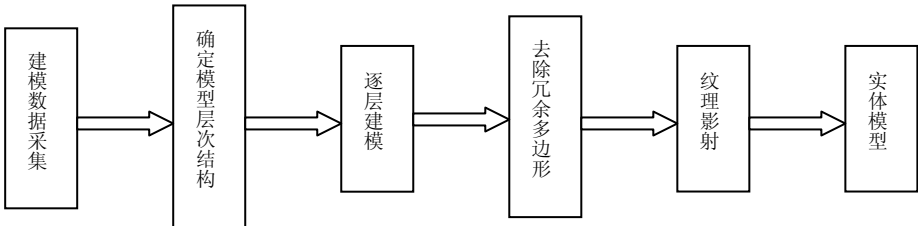


图 3 动态实体建模的一般步骤

3.2 基于“兴趣区域”的大规模地形数据库的分块调用

对高精度和真实地理信息方面的要求增加了仿真应用的复杂性。这样一次驻留在工作站内的数据库越来越大，也越来越复杂，即使目前最高档的图形工作站也难以承受，如何解决海量数据的管理问题是目前视景仿真领域研究的重点内容之一。

本文采用了基于“兴趣区域（AOI）”的大规模地形数据库分块调用技术来解决这一难题。如图 4 所示为模型分块调用过程。

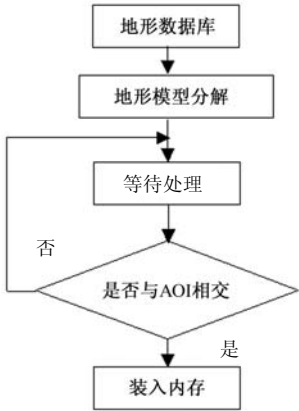


图 4 模型分块调用过程

3.3 典型碰撞检测和响应

碰撞检测及响应是视景仿真技术中一项非常重要的技术，是影响视景仿真系统逼真度和现实感的重要因素。本系统中涉及的碰撞检测及响应主要包括：炮弹（导弹）对目标或大地的碰撞检测及响应、运动目标与地形的碰撞检测及响应（地形匹配）以及视线的碰撞检测及应用等三个方面的问题<sup>[3]</sup>。

在碰撞及响应处理过程中，不同物体，碰撞检测的精度要求不同，响应处理的方法也不同。为此，为了提高碰撞检测及响应处理的速度及精度，本系统采用“独立节点处理法<sup>[4]</sup>”，即在视景显示模块中设立一个专门进行碰撞检测及响应处理的仿真单元，该仿真单元拥有较完整的碰撞检测及响应处理算法，当某个物体需进行碰撞处理时，先选择碰撞检测精度及响应处理方法，然后将该物体加入到对应的碰撞处理队列中。

### 3.4 视点控制与切换

视景仿真中的视点就是空间中观看某个局部（或全局）场景的某一个具体的位置，它控制着视锥体内的视觉表现，诸如观看什么，怎么观看。Vega 提供的基本视点方式分别是静止视点、运动模式视点、束缚视点（又包括跟踪束缚、固定束缚、旋转束缚三种）、规划路径视点。

在视点功能要求较高的视景系统中，仅仅采用 Vega 提供的基本视点方式及其组合已不能满足用户的观察需求。尤其是在大范围战场环境的视景仿真中，由于场景范围大、仿真实体多而且运动状态复杂多变，视点方式要求灵活机动，形式多样。为此，基于 Vega 视点的工作原理，我们设计开发了一种外设输入视点控制方式，它可以用鼠标、键盘等外部输入设备来灵活控制视点的运动和观看方向，调整出适合用户需求的最佳观看方式。

在视点转换方式的设计上，为了使视点切换时可以由一个位置平滑移动到另一个位置，避免了跳变，采用了线性插值的方式。控制面板中为每个仿真实体设定了按钮，单击可将视点的观察中心切换到所选物体上。系统还设计了键盘控制热键，用数字键和 SHIFT 加数字键可以快速切换观察物体。各种视点切换控制都可以通过可视化界面或键盘控制。

### 3.5 Vega线程与仿真线程的数据同步

炮兵作战指挥视景仿真系统，作为炮兵作战指挥仿真训练系统的一个联邦成员，与其他联邦成员是分布运行的，网络中的仿真数据和人机交互控制并不能直接用来驱动视景表现，视景系统通过内部自定义的消息类型来刷新场景，这就需要将网络中的仿真数据和人机交互信息转换成系统内部的表现命令，供视景显示模块识别并调用相应的操作。

分布式视景仿真系统在运行时采用了多线程的方式<sup>[5]</sup>，除了应用程序的主线程外，还有两个工作线程，即网络接口模块中 RTI 侦听线程和视景显示模块中实时视景渲染线程。这两个工作线程的工作流程如图 5 所示。这两个线程都属于工作线程，它们之间完全可以全局变量的方式进行通信。例如，当连观察所成员观察到敌装甲部队运动位置（x，y，z，）发生改变时，这个位置的数据信息被连指挥所成员所接收，并把这一数据交给已经定义了的用于线程通信的全局变量。视景线程会在每一帧的时间内实时检查这一数据，不管这一数据是否改变，它都会用这一全局变量来刷新一次视景内的敌装甲部队模型，当这一数据跟前一数据不一样的时候，那么刷新完成时，敌装甲部队的位置将位于新的坐标上，从而完成了远程数据的本地驱动。

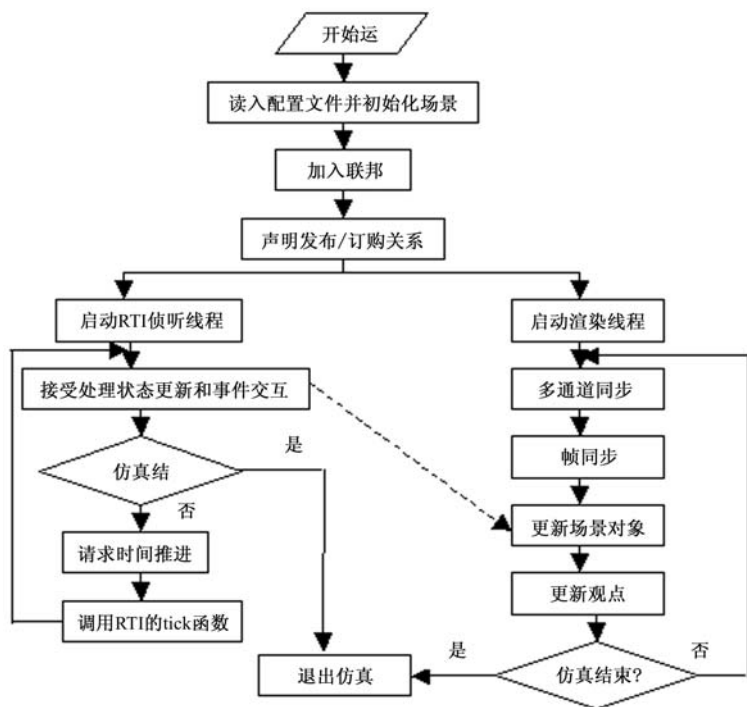


图5 RTI线程和Vega渲染线程的工作流程

## 4 系统演示

视景系统加入联邦后, 侦听态势显示系统中的实体配置信息, 并动态加载实体文件, 创建虚拟实

体对象; 然后开始侦听网络中对象类属性的更新和交互信息, 当接收到信息时, 虚拟实体负责根据接收到的交互类参数调用相应景况, 反映仿真中的事件。(演示略)

### 参考文献

- [1] 王海波, 等. 基于 HLA 分布式作战视景仿真系统开发[J]. 计算机仿真. 2005.9 (9)
- [2] 吴家铸, 等. 视景仿真技术及其应用 [M]. 西安. 西安电子科技大学出版社, 2001-7
- [3] 冯善达, 刘怡昕. 虚拟战场环境中典型碰撞问题研究[C]. 系统仿真学报, 2006.6
- [3] 康凤举. 现代仿真技术与应用[M]. 北京. 国防工业出版社, 2001-9
- [4] 甘斌, 等. 一种可重用的视景邦员设计与实现[J]. 计算机仿真. 2006.4 (4)

### 作者联系方式

通信地址: 济南经十一路 80 号通信部信息化工作办公室

邮政编码: 250002

联系电话: 0531-51685630

# 机载VLF中继通信系统探究

李俊清

**摘 要:** 本文介绍了机载 VLF 中继通信系统的通信特点、系统组成、有关性能指标和关键技术,并对系统的通信性能进行了初步分析。

**关键词:** 对潜通信; VLF 通信; 机载中继通信系统

## 1 引言

战略核潜艇是世界上公认的最具威慑力的二次核打击力量。但它在执行战略反击任务时,必须有安全可靠的通信保障来提供支持,否则难于完成其使命。目前,常用的通信方式主要是靠 VLF/SLF 频段通信实施的。工作在这些频段上的岸基大功率发信设施的复杂、天线结构庞大,存在着抗毁能力差而且破坏后难以恢复的缺点。在未来的战争中,它们必定是敌方以精确制导武器首先摧毁的目标。因此,这就向我们提出了当发生这种情况时,如何保持与核潜艇通信联络的问题。考虑到未来信息化战争的特点以及需确保与战略核潜艇通信联络的要求,需要有一种具备较强顽存能力的应急通信手段,以在岸基 VLF、SLF 大功率发信台遭到破坏后能代替其工作。机载 VLF 中继通信系统就是可提供这种顽存性应急通信能力的一种最佳选择。美国、俄罗斯(前苏联)早在上世纪六、七十年代就研制了这种通信系统,而且经过几十年的应用和多次改进提高,迄今为止,仍把它作为对核潜艇实施抗毁应急通信的主要手段。

进入 21 世纪后,为了完成新时期赋予我国海军的任务,作为“杀手锏”的战略核潜艇有了新的发展,而且对其完成使命的能力有了新的要求。因此,无论是从发展我国海军战略指挥通信的角度,还是从确保我国战略核潜艇具有最低限度应急通信能力的需要,都应考虑发展建设我国海军的机载 VLF 中继通信系统。

本文分别介绍了机载 VLF 中继通信系统的通信特点、系统组成、系统主要性能和关键技术的有关情况,并就可能实现的机载 VLF 中继通信系统的性能作了初步分析。

## 2 通信特点及系统组成

### 2.1 通信特点

这种系统用 VLF 电磁波作为对潜中继的手段,众所周知,VLF 电磁波具有三个独特的优点:一是它可以穿透海水,能使潜入水下的潜艇接收信号;二是它的传播距离远,基本上可实现全球范围的通信;三是它在严重的大气干扰情况下亦能良好传播并具有一定的抗核爆炸电磁脉冲的能力。因此,VLF 电磁波一直被用作对潜通信的主要手段。但是,在战争期间,尤其是发生核冲突时,岸基 VLF 大功率发信设施由于体积庞大,目标显著固定而很容易被敌方摧毁。陆基车载式机动 VLF 发信系统又因为其发射功率和天线高度受到较大的限制,无法满足远离本土的潜艇,尤其是无法满足战略核潜艇执行任务时的通信需要。机载 VLF 中继通信系统则在一定程度上克服了两者的不足,它不但具备较强的顽存能力,而且也有较强的通信能力。机载 VLF 中继通信系统把 VLF 发射设施及配套的中继通信设备直接安装在专用的运载飞机上;当任务需要时,载机可立即升空并飞行到相关空域,随后放出天线,把中继信息及时转发给正在执行任务的潜艇。这种机载系统行动灵活、机动性强、便于临时行动、有较强的顽存能力;而且由于系统的辐射效率较高,十分适合用作核潜艇战略指挥通信的应急手段。

在向核潜艇发送信息时,这种系统通常是以单向通信方式工作的。它从国家指挥当局或其他指挥机构获取命令与信息(上行链路),而向潜艇转发 VLF 报文信息(下行链路)。为可靠起见,它可有多条上行链路,所用频段可从 VLF、HF 到 UHF,

甚至可接收 EHF 卫星信息。所有上行链路可用来传送相同的关键报文以确保正确的接收。而且很重要的一点是,它可在接收多种频率的低电平信号的同时,能在存有干扰的环境下用大功率发射 VLF 信号。

## 2.2 系统组成

机载 VLF 中继通信系统的原理框图如图 1 所示。

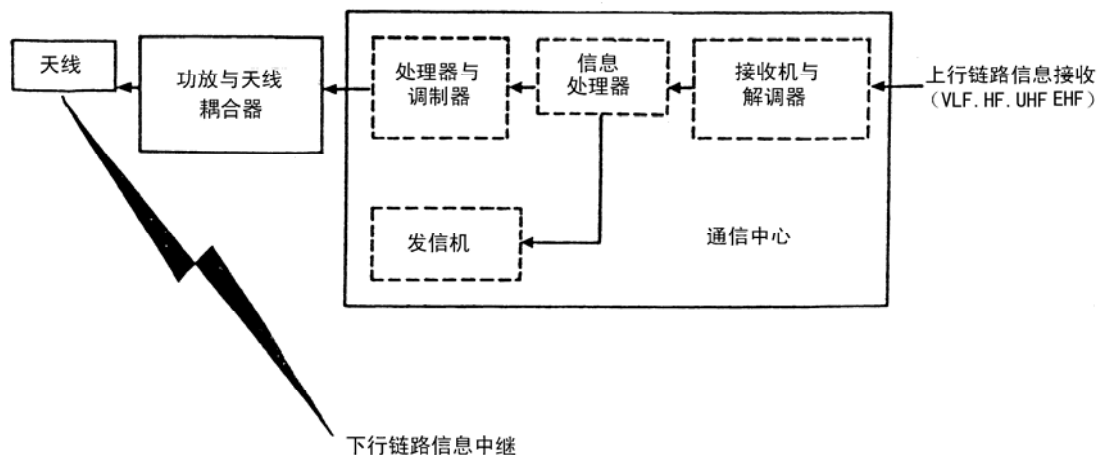


图1 机载 VLF 中继通信系统的原理框图

系统主要由三部分组成,即:①通信中心与接收机/发信机的组合体;②VLF 功率放大器、天线耦合器以及双线式 VLF 拖曳天线;③系统的载机。下面对其中有关部分做一简单介绍。

### 2.2.1 通信中心组合体

它主要包括下述系统与设备:

- VLF 发射和接收系统
- HF 和 UHF 接收机/发信机、调制器和控制器(可增加有 EHF 接收单元)
- 系统信息处理系统
- 内部通信系统
- 辅助控制和监视设备

系统可用各种调制方法和保密的或非密的方式在很宽的频率范围内接收和解调上行链路的信息,主要采用的方式有:

- VLF——扩频、MSK、FSK、CW
- HF——话音、FSK 和 CW
- UHF——卫通信号及视距话音
- EHF——卫通信号

系统接收到的报文先输入到系统的信息处理部分,用以进行报文加密、优先级识别、分类、格式化、显示、文本编辑和存储。利用计算机辅助的显示/键盘终端,载机上的通信人员可控制路由选择并把报文发送给选定的 VLF/HF/UHF 发信机。当对潜艇进行中继通信时,中继报文先发送给 VLF

数字信息网的发射端,用来进行抗干扰的 MSK 编码调制及加密后再行发出。

### 2.2.2 VLF发射分系统与发射天线

VLF 发射分系统是中继通信系统的重要组成部分,也是该系统比较独具特色的部分。它用载机所拖拉的天线向潜艇发送报文,形成下行链路信息中继信道。分系统的组成示意图如图 2 所示。

发射分系统的原理框图如图 3 所示。

其中,VLF 功率放大器与耦合器的作用是把 VLF 发射信号放大到 200kw 的功率并完成大功率信号与拖曳式双线天线的耦合。系统所用的 VLF 发射天线是由长天线和短天线组成的双线式拖曳天线,载机上装有天线专用的收发装置并可由载机上放出。其中长天线一般长约 8000 米(长度的选择视工作频率而定),其由装在尾舱前部的鼓轮穿过机身地板放出;短天线可起补偿和平衡的双重作用,它由尾翼前边缘处的后机身放出,一般约为 1200 米。两天线的末端都装有平衡锥袋,供飞行时保持天线状态的稳定。当系统向潜艇中继信息时,载机放出天线并按一种精心控制的园形轨道飞行。这样做的主要目的是为了使长天线在飞行时具有较大的垂直度(一般要求垂直度>70%),以便获得更高的垂直有效辐射功率。

机载甚低频（VLF）发射系统

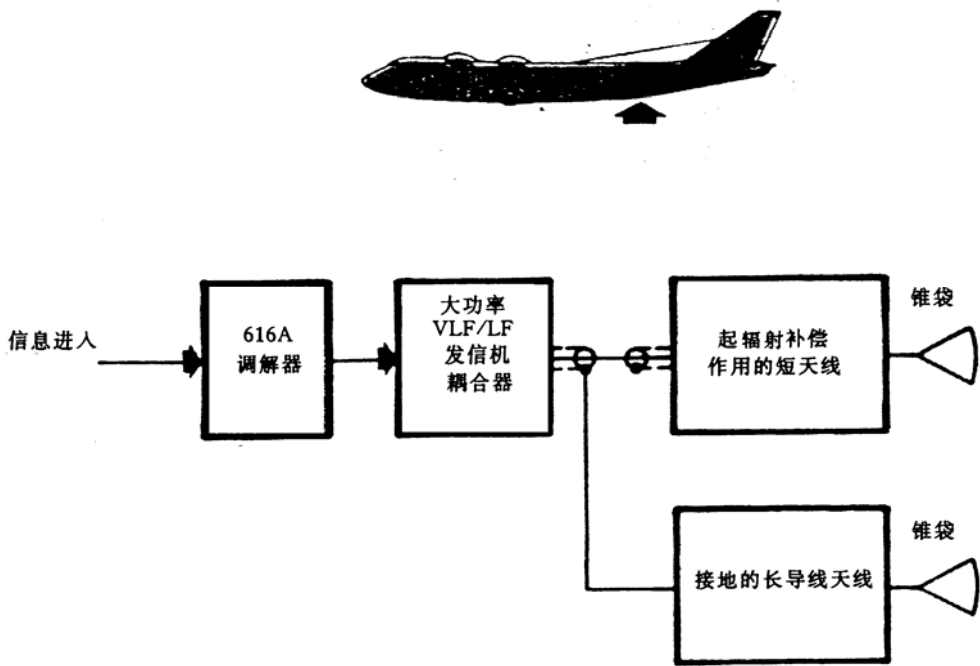


图 2 VLF 发射分系统组成示意图

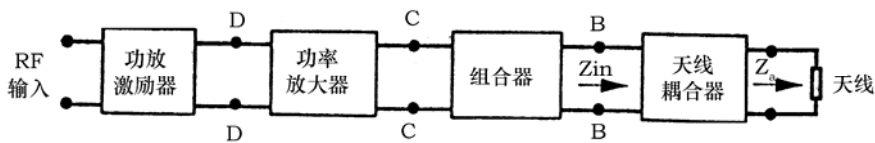


图 3 发射分系统原理框图

2.2.3 系统载机

对系统载机的基本要求是：① 应能在与任务相适应的空域中飞行；② 续航力要强；③ 要有足够的承载能力；④ 要有足够的飞行速度。小型飞行器，如直升机、无人飞艇等是无法满足这些要求的。因此，一般都是选用有固定翼的、多引擎的运输机或客机改装而成。上世纪八十年代之后，美国海军选用的是在波音 707 型客机的基础上改装而成的系统载机，即“E—6”型飞机，前苏联（俄罗斯）则用的是由图—142 型飞机改装而成的“Beer-J”型飞机。

美 E—6 型飞机的机载设备配置情况见图 4 所示。

3 主要性能与关键技术

3.1 机载VLF中继通信系统典型的技术性能

- 上行链路工作频段：VLF、HF、UHF 及 EHF
- 下行链路（对潜）工作频段：VLF（14～30kHz）
- VLF 发射机功率：200kw
- VLF 发射天线效率：50%
- VLF 发射天线收放时间：<45 分
- 文电处理系统功能：自动完成优先级识别、分类、格式化、显示、文本编辑、加解密处理、存储和分发控制等。

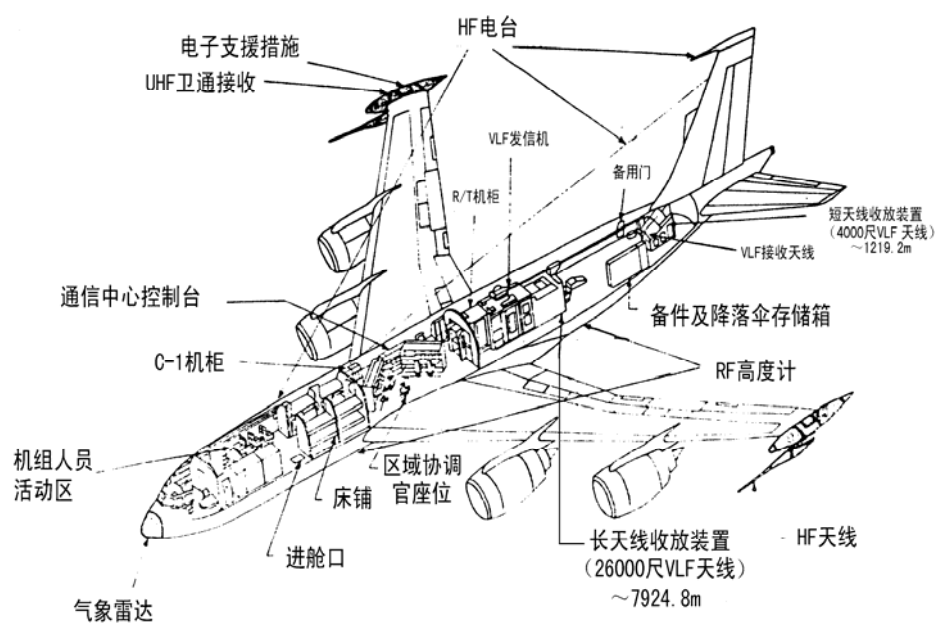


图4 美E-6型飞机的机载设备配置图

3.2 研制机载VLF中继通信系统需解决的主要关键技术

- 系统总体设计与集成技术
- 机载 VLF 拖曳天线与收发装置的设计研制
- 机载 VLF 固态大功率发射技术
- 载机飞行姿态控制技术
- 载机改装设计与相关的电磁兼容技术
- 机载大功率电源技术

4 通信性能简要分析

表 1 列出了机载 VLF 中继通信系统与常见的陆基车载 VLF 机动台和陆基固定大功率 VLF 发信台一般标称性能的比较情况。由表中数据可以看出，机载 VLF 中继通信系统在天线辐射效率、通信距离及顽存能力方面有一定优势。下面重点对三者的通信距离进行简单的比较分析。

表 1 性能比较表

	车载 VLF 台	机载 VLF 系统	陆基大功率 VLF 台
发射机功率 (kw)	100	200	2000
天线辐射效率	百分之十几	50%	30%
辐射功率 (kw)	十几	100	600
通信距离	近	远	远
顽存能力	较好	好	差
费 用	低	高	高

从表中列出的基本数据可以看出，车载机动台因为发射机功率受到限制（100kw 及以下），而且由于所用天线的垂直高度一般不大于 2000 米，天线辐射效率仅有百分之十几，因此有效辐射功率也只有十几千瓦；再加上所用的机动车辆只能在本土上移动，因此，其通信距离较近，一般无法满足战略核潜艇执行任务时的通信需求。

机载 VLF 中继通信系统的发射天线长度可接近工作频率的 $\lambda/2$ ，天线辐射效率可达 50%以上，当机载 VLF 发射机的功率为 200kw 时，其有效辐射功率可达 100kw。尽管这种辐射功率与陆基大功率台的辐射功率（600kw）相比要低 7.8dB，但它可通过另外两种因素来加以补偿。其一是机载 VLF 中继通信系统的载机在目前情况下可在航空兵有制



空权的近海海域机动飞行。这对可能的与核潜艇的通信距离而言,其可相当把目前的陆基 VLF 大功率发信台向海洋推进了近 1500 公里。已知 VLF 电磁波在混合路径(20%陆地,80%海洋)上的损耗值约为 3dB/千公里,这种距离的推出,可得到大约 4.5dB 的功率补偿;其二是,如果考虑到在紧急通信情况下可允许 VLF 通信的传输速率比正常情况降低一倍的条件,那么由此至少又可获得 3dB 以上(最高可达 5dB)的增益。把这两种因素综合在一起考虑,可以看到,把机载 VLF 中继通信系统作为最低限度应急通信手段时,其通信能力基本上与目前国内的 VLF 大功率发信台相当。如果将来随着我国海军航空兵装备的进一步发展,我军具有了中、远海域的制空权,那么机载 VLF 中继通信系统完全可以超过陆基 VLF 大功率发信台的通信能力,这样就可支持核潜艇到更远的海域执行任务,从而使其具备更大的威慑能力。另外,需要指出的是,这种系统不但可用于海军的战略通信,其平时作为海军 VLF 战术通信的备用手段也是十分有效的。

## 5 结语

机载 VLF 中继通信系统具有较好的对潜 VLF 通信能力,而且机动性高、灵活性大、使敌方难以实施预先的精确打击,在作战环境下具有较强的顽存能力,因此可作为未来战争(包括核冲突)中确

保对核潜艇实施作战指挥的应急通信手段。

美国、俄罗斯(前苏联)发展应用机载 VLF 中继通信系统的多年实践证明:该系统与极(超)低频对潜通信系统配合使用,完全可以使弹道导弹核潜艇在海洋的最佳深度上与岸基指挥部保持良好的连通,因而可为核潜艇执行任务提供隐蔽安全的环境。在极(超)低频系统和主要指挥部受损的恶劣情况下,机载 VLF 中继通信系统亦有可能带着临时指挥部发出的紧急行动报文(EAM)去完成对执行任务的核潜艇的指挥通信。

美国海军研究人员经多年研究认为:目前还没有哪一种在役或在研的类似系统能像机载 VLF 中继通信系统那样具有可适应战争威胁变化的抗毁性和灵活性。正因为如此,美、俄等国仍把该系统作为其对核潜艇战略通信的主要应急手段,而且一直不断地对其改进完善。

为了应对未来复杂多变的国际形势及祖国统一大业的需要,发展我国的机载 VLF 中继通信系统亦应提上议事日程。当然,我国要研制这样的一种系统,会遇到技术难度和投资较大、长期维持需有较大的人力、物力保证的问题。不过根据我国现有的经济实力和技术发展水平,再考虑到正在发展的 SLF 系统的情况,应当说通过借鉴国外比较成熟的系统与技术,结合我国国情,在近期内研发一种适合我国核潜艇应急战略通信需要的机载 VLF 中继通信系统也不是没有可能的。

## 参考文献

- [1] “Talking to submarines”, JANE'S DEFENCE WEEKLY, 1984
- [2] “An examination of the complex TACAMO communication system—the manned communication relay link to the strategic force”, SIGNAL, 1978
- [3] 海军战略指挥通信系统, 722 所研究报告, 2002
- [4] 海军舰船通信系统, 内部译文集, 1996

## 作者联系方式

通信地址: 武汉市 70005 信箱中国船舶重工集团公司第七二二研究所系统技术部

邮政编码: 430079

联系电话: 027-67889521 13507199543

# 基于遗传算法的多Agent信息过滤系统研究

李双 赵怀勋 赵方舟

**摘 要：**针对网络军事信息搜集的需要，设计了一种基于遗传算法的多 Agent 军事信息过滤系统。系统在传统搜索引擎基础上，采用遗传算法和用户反馈建立并更新用户模型、多 Agent 交互协作的方法来实现情报信息的过滤，实验证明了该算法的有效性。

**关键词：**军事信息过滤；Agents；遗传算法；显式反馈

## 1 引言

随着全球互联网的迅猛发展，导致了军事信息的日益透明化。网络的普及使军事信息遍布世界各地形形色色的网站中，为网络情报信息搜索带来了契机的同时也带来了问题，即所谓的“信息过载”（*Overabundance of Information*），传统的搜索引擎虽然解决了资源定位问题，但仍不能满足人们对信息质量日益增长的需求<sup>[1]</sup>。例如在 Google 中输入关键词 *cold war*，查询到的网页已经超过七千万，从中遴选出实用信息无异于大海捞针。信息过滤技术则是对搜索引擎的有效补充，它可以识别无用信息并能主动向用户进行信息推荐，因而在军事情报搜集过程中有着显著的研究利用价值。

如何进行用户建模和选择过滤算法是信息过滤的关键问题，本文设计了一种基于遗传算法的多 Agent 军事信息过滤系统（以下简称 MIFS），在用户提供显式反馈的条件下获取用户兴趣，从而帮助用户准确获取有价值信息，以满足军事网络信息检索的需要。

## 2 系统设计

### 2.1 系统的结构

由于反馈的存在，智能技术和机器学习的方法已经在信息过滤系统中得到广泛的重视。Agent 的自治、社会、反映、主动、学习等特征以其极大的灵活性和适应性，使之更加适合于开放、动态的网络环境。将多 Agent 技术应用于信息过滤，能够克服无智能检索的弊端，而且对于特定的任务能产生较好的过滤结果。

多 Agent 军事信息过滤系统的模型如图 1 所示，系统通过用户模型（*User Profile*）来描述用户的信息需求。Agent 围绕用户模型进行功能分配：用户 Agent、学习 Agent 和过滤 Agent。

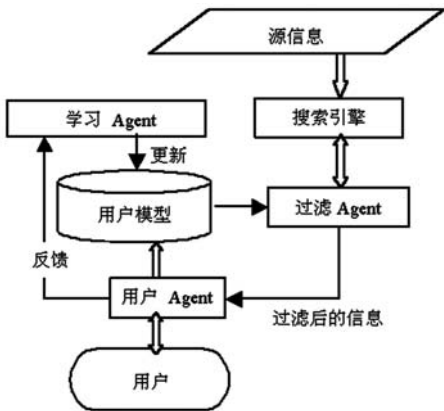


图 1 军事信息过滤系统(MIFS)的模型

系统的具体流程如下。

- 1) 用户 Agent 从系统用户那里得到用户针对军事情报主题的惯用关键词（*Customary Key Words*），并将这些关键词保存到用户模型（*User Profile*）中，作为初始化的用户模型；
- 2) 过滤 Agent 从用户模型中提取查询关键词，将得到的查询关键词送往搜索引擎；
- 3) 搜索引擎把从 Internet 检索的结果返回到过滤 Agent；
- 4) 过滤 Agent 通过特征匹配将过滤得到的的结果传送到用户 Agent；
- 5) 用户 Agent 将 4) 得到的过滤信息呈现给用户并记录下用户对信息的反馈（*Feedback*），继而将这些反馈信息送往学习 Agent；
- 6) 学习 Agent 根据上一步得到的用户反馈信息计算出用户对多 Agent 系统过滤结果的满意度（*Utility*），并根据满意度更新用户模型；

7) 返回。

## 2.2 Agent功能描述

MIFS 的三个功能 Agent 彼此独立又相互协作, 其具体描述如下。

1) 用户 Agent: 用户 Agent 是一个界面 Agent, 负责与用户交互, 主要由输入、输出和反馈提取三者所构成, 用户通过界面进入 MISF 的查询界面, 在查询界面中用户可以选择自己感兴趣的主体类别, 输入查询关键词进行查询。用户 Agent 可以主动的探测环境变化, 包括用户行为, 并根据用户反馈来扩展用户。

2) 过滤 Agent: 过滤 Agent 通过搜索引擎来搜索信息, 从返回的网页中删除 html 标记、脚本语言、数字等一些没有实质意义的标识后, 通过特征提取选出文本特征词和用户模型中的关键词进行匹配来决定取舍。需要提出的是, 考虑到覆盖率和实用性, 本文提出的多 Agent 军事过滤系统主要处理的是英文信息。

3) 学习 Agent: 学习 Agent 负责学习用户的反馈, 根据用户的满意度可以得出用户对系统过滤结果的满意程度, 然后调整相应的关键词的权值来更新用户模型。

## 2.3 用户模型的描述和更新

本文采用的是向量空间模型 (VSM), 即用向量来表示文本, 用  $d$  (Document) 表示; 特征项是指出现在网页  $d$  中且能够代表该网页文本内容的基本语言单位, 用  $t$  (Term) 表示, 主要是由单词或者词组构成。文本可以用特征项集来表示  $d(t_1, t_2 \dots t_n)$ , 例如网页的文本信息通过排除那些没有任何实质意义的代词 (i.e. *we*、*here*、*it*)、形容词等, 剩下的关键词就可以视为该文本的特征项。 $n$  即为向量的维数, 向量的每个分量对应于关键词的权值  $w$ , 用以表示特征项对于文本内容的重要程度。网页文本信息  $d$  和用户模型  $p$  之间的相似度用它们之间夹角的余弦来衡量<sup>[1]</sup>。其表达式为:

$$Sim(d, p) = \cos(d, p) =$$

$$\frac{d \cdot p}{\|d\| \|p\|} = \frac{\sum_t w_{t,d} w_{t,p}}{\sqrt{\sum_t w_{t,d}^2} \sqrt{\sum_t w_{t,p}^2}}$$

利用余弦相似法计算网页文本信息  $d$  与用户模型  $p$  之间的相似度, 并把结果大于阈值  $T$  (Threshold Value) 的网页传送给用户 Agent, 学习 Agent 通过用户的反馈来及时更新 User Profile 中关键词的权值。

## 3 Agent学习算法的实现

### 3.1 遗传算法

遗传算法 (Genetic Algorithm) 最初由美国 Michigan 大学的 J.H.Holland 提出来的, 其本意是在人工适应系统中设计的一种基于自然演化原理搜索机制<sup>[2]</sup>。遗传算法将问题的求解过程看成是一个在候选解空间中寻找满足问题要求的解或最优近似解的求解过程, 其重点在于适应规划和适应度量方面, 适应规划用于指导怎样在解空间进行搜索, 一般采用遗传算符 (选择、交叉、变异等); 适应度量采用计算适应值的方法来评价一个候选的优劣。在遗传算法中, 每个个体根据解决的问题好坏被赋予一个适应值, 适应度高的个体有更高的机会通过和其他个体“交叉繁殖”进行再生。那些适应度较低的个体因为不太可能被选来再生, 最后都会“灭绝”。遗传算法流程如图 2 所示, 其中  $G$  为遗传代数,  $i$  为进化中新形成个体的个数,  $N$  为群体规模。

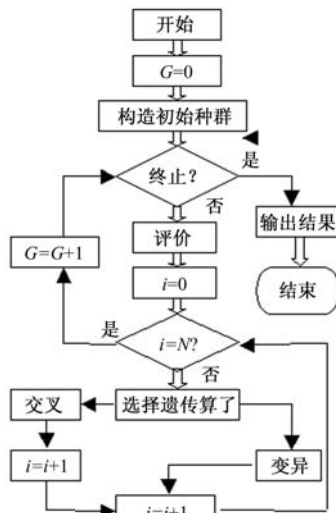


图2 遗传算法的流程

### 3.2 基于遗传算法的Agent学习

学习 Agent 的功能在于根据用户对军事情报信

息收集的需求，采取某种学习方法来逐步明确用户兴趣，实际上它是一个机器学习的过程，我们采用遗传算法来学习和适应以判断对关键词的选择和组合。用户对过滤结果通过用户 Agent 进行评价反馈，用于改进 Agent 的学习过程。

学习 Agent 通过遗传算法寻找最优特征选择方案，算法收敛后，将得到最佳的关键词（可能是英文单词也可能是词组）集合。具体算法如下：

```
Procedure 基于遗传算法的 Agent 学习
Begin Initial(); /*产生最初的 N 个关键词的种群;
while 不满足群体收敛条件 do
    Begin For 群体大小/2 do
        Fitness(); /*根据系统的过滤效果评价个体的适应度;
        Selection(); /*从旧代中选取两个适应度较高的个体进行繁殖;
        Crossover(); /*交叉，重组这两个个体来产生两个后代;
        Mutation(); /*变异;
    End;
End;
```

遗传算法构造出的种群由若干个关键词（个体），并把若干个关键词结合起来表示用户模型，同时发现新的相关主题，通过搜索引擎找出与此相关的页面，并根据用户的反馈及时地调整关键词的权值，从而加速这种学习过程。

3.3 遗传运算的操作

(1) 选择 (Selection)

从种群中选择出较适应度好的个体。这些选中的个体用于繁殖下一代。有时也称这一操作为再生 (Reproduction)。选择用于繁殖下一代的个体时，据个体对环境的适应度而决定其繁殖量的，故也称为非均匀再生 (Differential Reproduction)。

(2) 交叉 (Crossover)

交叉运算是取两个关键词集合，随机地在某一点上分开，然后重新组合形成两个新的关键词集合，重新安排染色体的基因，新的染色体由于继承了父染色体的优良特性，因而要优于上一代。但传统的交叉算符要加以修改才能使用，否则有时会形

成不合理的表示。一般来说，当且仅当相同的词在所有新的关键词种群（遗传算法中称之为染色体）出现不超过一次时，交换所有的关键词。

(3) 变异 (Mutation)

变异操作有两种：一种是从种群中选出两个染色体，当且仅当相同的词在每个染色体中出现不超过一次时，在某一选定的点上交换它们各自的关键词。第二种方法是从种群中选出一个染色体，在某一选定点上将其关键词与词典中的关键词进行交换。最后，从种群中选出最合适的染色体组成新的种群，如此循环反复，直到生成一定数目的后代。

3.4 实验及结果分析

为了检验遗传算法对 Agent 学习的有效性，我们从军事专刊<sup>[3]</sup>中抽取语料，挑选出 64 个单词作为训练样本。采用简单编码方式，即用 1 个 N 位的 0 或 1 构成字符串表示一个关键词组合集，其中 1 所对应的关键词被选中，0 所对应的关键词未被选中；随机产生一系列字符串作为初始种群。用户反馈（满意度）调整个体适应值，遗传算法在 100 代后终止，交叉概率为 0.5，变异概率 0.01。算法终止后，得到的一组选取出现次数最多的为最终的关键词选择方案。

将算法运行 50 次，每次得到 1 个最优子集，累计 50 次结果后进行归一化处理，得到选中率最高的 8 个关键词，初始权值采用比较普遍的 TF-IDF 方案。选中关键词的初始权值和训练后的权值如表 1 所示。可以看到作为用户模型里的关键词经过训练后，相应的权值有着明显的改善，更能体现关键词对相应信息的重要程度。其中，military 和 warfare 虽然词频高，但是在军事报告中并没有表达实际含义，所以权值在进化后明显变低，其余的 56 个词由于适应度太低被“淘汰”。同时降维处理后，需要匹配的特征项减少，过滤速度也会随之提高。

表 1 选中关键词 (SK) 的初始权值 (OW) 和修正权值 (MW) 比较

SK	gas turbine	naval	weapon	military
OW	0.01	0.06	0.05	0.12
MW	0.07	0.12	0.09	0.05
SK	Anti-satellite	warfare	BADGE	pilot
OW	0.01	0.07	0.03	0.02
MW	0.08	0.03	0.10	0.04

实验结果表明,利用遗传算法,学习 Agent 可以针对用户的显式反馈,及时调整关键词的权值来更新用户模型。对比固定的用户模型而言,有着比较好的环境适应性。

## 4 结束语

本文设计的基于遗传算法的多 Agent 军事信息过滤系统,适用于 Internet 上的智能军事信息搜索。与其他过滤系统相比<sup>[4]</sup>,本系统的不同在于用户群体的特殊性,它可以对政府、军事、安全部门的网站的信息进行追踪,对其他网站曝光的军事信息进行鉴别和过滤。其优点在于可以自主地进行更

新用户模型。然而,该结构下系统的实现面临着一些难点问题,突出表现为 Agent 间的通信、信息的有效提取和提高过滤的扩展率等问题,这也是国外自动信息搜集研究领域亟待解决的问题<sup>[5]</sup>,这些研究的进展势必将为系统的进一步实用化作好铺垫。

另外需要指出的是,本文讨论的军事信息过滤实质上是一个信息推荐的过程,如何保持过滤算法的稳定性,提高信息推荐的质量以及从过滤的信息集合中发掘潜在的隐含信息同样应该纳入考虑范围<sup>[6]</sup>。当然,建立一个动态网络中的高可信度的自动情报生成系统也正是我们研究军事信息过滤的目标。

## 参考文献

- [1] Panagiotis Petratos. Information Retrieval Systems:A Human Centered Approach. Interdisciplinary Journal of Information, Knowledge, and Management.2007, 2:17-32
- [2] 张文修,梁怡.遗传算法的数学基础.西安交通大学出版社,2000.5
- [3] United States Naval Institute Proceedings with Annual Naval.2007, 3 (133)
- [4] SEO Y-W, ZHANG B-T. Personalized Web-document Filtering Using Reinforcement Learning. Applied Artificial Intelligence, 2001, 15 (7) : 665-685
- [5] Bernard J. Jansen, Tracy Mullen etc. Automated gathering of Web information. ACM Transactions on Internet Technology, Vol. 6, No. 4, November 2006:442-464.
- [6] Jonathan L.Herlocker, Joseph A.Konstan etc. Evaluating Collaborative Filtering Recommender Systems. ACM Transactions on Information Systems, Vol. 22, No. 1, 2004, 1:5-53
- [7] Yi Ding, Xue.Li. Time Weight Collaborative Filtering. CIKM'05, Oct31-Nov5, Bermen, German, 2005:485-492

## 作者联系方式

通信地址:陕西省西安市武警工程学院研究生三队

邮政编码:710086

联系电话:13572431715 029-84563623

# 军事信息资源开发利用中数据标准化建设问题

李晓 冯骞

**摘 要:** 本文针对我军信息资源开发利用的关键——数据标准化建设进行了深入的论证, 提出数据标准化建设的主要内容和建设思路

**关键词:** 信息资源; 开发利用; 数据建设; 标准化

数据是信息资源的主要表现形式, 是信息资源开发利用的基础。准确、规范的数据, 即标准化数据是信息资源开发利用的必备条件。近年来, 军队陆续开展的一些信息资源建设工程中, 数据标准不统一问题已成为制约工程建设质量的“瓶颈”, 引起各方的严重关注。本文就军事信息资源开发利用中数据标准化建设问题做一些探讨。

## 1 数据标准化的界定

目前, 理论界对数据标准化的界定还没有形成统一的共识, 有关专著中对数据标准化的概念有各种各样的描述, 这些定义基本上是从民用信息资源管理角度出发的, 结合军队信息资源开发利用实际进行准确描述的还没有。参考有关理论书籍, 借鉴军队信息资源工程建设经验, 笔者认为军队数据标准化建设是指以军队信息资源开发利用环境为依托, 以数据标准制定、颁发、管理为重点的组织管理过程, 主要包括标准化建设环境和数据标准建设等。标准化建设环境即数据标准的制定、发布、管理的相关机构、部门以及执行、落实、监督的有关制度; 数据标准化建设即数据采集、存储、交换与更新的具体标准。

数据标准化建设环境建设是军事资源开发利用工作的重要保证和基础工程。目前, 我军信息资源开发利用标准化建设环境已有初步基础, 设有信息化建设领导小组和日常工作办公室, 统筹组织、管理信息资源开发利用的建设工作和起草、发布标准规范和执行、落实、监督情况。几年来, 各级信息化组织管理机构起草、制定了信息化建设的有关工作条例, 颁发了相关技术体系结构, 梳理、规范了作战信息资源需求论证和政治、后勤、装备信息化建设标准, 启动了数据工程建设和武器装备信息化

改造, 组织开展了相关学术理论研讨活动, 培养了一批信息化建设和信息资源开发利用人才骨干。这些工作和成绩, 为我军进一步开展信息资源建设和深化军队建设转型奠定了坚实基础。

数据标准是数据标准化建设的重点和实质内容。我国信息资源规划专家高复先教授认为信息资源开发利用中需要统一的数据标准是“信息资源管理基础标准”, 它是建设好数据中心, 确保信息资源共享和各种数据流自动化畅通的基础, 包括数据元素标准、信息分类编码标准、用户视图标准、概念数据库标准和逻辑数据库标准等, 军队必须统一数据标准, 其根本目的是: 为实现互联互通、信息共享、业务协同、信息安全打好基础, 确保信息资源开发利用的高水平、高质量和高效率。军队信息资源开发利用的特点和建设任务决定了建立完善的数据标准化体系是非常重要的基础工作。

美国学者威廉·德雷尔在 1985 年出版的专著《数据管理》一书中, 对数据标准化进行了深刻的阐述, 他的名言是: 没有卓有成效的数据管理, 就没有成功高效的数据处理, 更建立不起来整个企业的计算机信息系统。威廉提出了一些数据标准化建设的重要原则。

1) 不能把例外当成常规。任何原则都有例外的情况, 没有适用于所有情况的标准。但是, 数据管理人员决不允许把例外当成常规。

2) 管理部门必须支持并乐于帮助执行标准。如果违背了标准, 管理部门必须帮助确保那些违背标准的行为得以纠正。

3) 标准必须是从实际出发、有生命力、切实可行的。标准必须以共同看法为基础, 标准中复杂难懂的东西越少, 就越好执行, 要保持标准的简明性。

4) 标准决不是绝对的, 必须有某种灵活的余

地。尽管有些标准必须严格遵守，但是大多数标准不应该严格到束缚数据设计人员的灵活性的程度。

5) 标准不应该迁就落后。标准要控制和管理当前和未来的活动，而不是恢复和重演过去的做法。

6) 标准必须容易执行。要达到这一点，必须容易发现违反标准的情况，能自动检查标准符合情况的方法愈多，标准本身愈加有效。

7) 标准必须加以宣传推广，而不是靠强迫命令。即使上级主管部门完全支持数据管理标准，也要向各级业务人员宣传这些标准。任何持久的、有意义的变化必须来自员工自己对标准的认识。

8) 标准的细节本身并不重要，重要的是有某些标准。数据管理人员必须善于综合考虑和商讨所要制定的标准细节。

9) 标准应该逐渐制定出来，不要企图把所有的数据标准一次搞完。标准一旦制定出来，就要开始执行，但执行标准是一个渐进的过程，而不是突变的过程。

10) 数据管理的最重要的标准是一致性。数据命名、数据属性、数据设计和数据使用必须一致。

这十条原则虽然是针对企业信息化建设提出的，但今天看来，对我军数据标准化建设也有很好的启发和借鉴意义。

## 2 数据标准化建设的内容

当前，军队数据标准化建设存在某些盲目性和片面性，如标准化建设搞得很空，不适用的“标准”罗列了一大堆，过于烦琐的“标准”没法用，关键性的数据标准没有得到充分的重视；数据标准的制定缺乏系统的考虑，仅限于数据元素标准和编码标准，而忽视了对用户视图和数据库的标准化建设。这些问题的出现，主要原因是没有深入分析军事需求，即复杂的数据流和数据关系。数据流是数据库设计的基础，主要是从作战指挥数据保障的角度，描述需要的数据及其组成与分类，规定数据信息范围，描述用户概念上的数据项集合及数据项间的相互关系，以及每个数据项的说明等。

理清复杂的数据流，建立统一的数据标准，是确保信息资源共享，实现信息资源整合的基本工作。

借鉴理论研究成果和联合共享数据库建设实践，军队信息资源开发中数据标准化内容主要包括以下五个方面。

1) 数据元素标准。数据元素是最小的不可再分的信息单位，是一类数据的总称。在对数据元素进行创建和命名时，可以借鉴对化学元素（共有100多个）的研究，把握其有限数目的“核心”数据元素，这就需要建立数据元素命名标准、标志标准和一致性标准。如“通信装备编号”，其命名结构为“修饰词—基本词—类别词”，“通信”是修饰词，“装备”是基本词，“编号”是类别词，对修饰词、基本词、类别词进行替换，可以得出诸如“电子对抗装备编号”、“通信人员编号”、“指控装备性能”等等众多符合统一命名规则的数据名称。

2) 信息分类编码标准。信息分类编码标准是在信息分类的基本上将信息对象赋予有规律的，能让计算机和人易于识别与处理的符号。主要包括识别编码对象、研制编码规则（遵循已有的国际标准、国家标准和军队标准）和编制出代号表。如联合共享数据库，将信息分为为二级，即十大类49项。

3) 用户视图标准。用户视图是一些数据的集合，它反映了最终用户对数据实体的看法，包括单证、报表和屏幕格式等。用户视图会起到“左右”、“上下”、“内外”数据流载体的作用。在网络环境中以屏幕格式取代大量的报表，这就必须做好简化和标准化工作。

4) 概念数据库标准。概念数据库是最终用户对数据存储的看法，是对用户信息需求的综合概括。简单说，概念数据库就是主题数据库的概要信息。

5) 逻辑数据库标准。逻辑数据库是对概念数据库的进一步分解和细划，一个逻辑数据库由一组规范化的基本表构成，基本表是规范化的理论与方法建立起来的数据结构。

上述五项数据标准是紧密联系、不可分割的统一体，共同构成了军队信息资源管理基础标准体系，是标准化建设的重要内容。没有这种数据标准化体系，各级数据中心和信息资源库就不能成功建设，各种业务应用系统就不能实现信息共享和高效运作。

### 3 数据标准化建设必须结合信息资源规划进行

军事信息资源开发利用工作是一项复杂的系统工程,数据标准化建设是这项系统工程中的基础性工作,是总体设计即信息资源规划中的顶层工作。钱学森同志在《论系统工程》中特别强调总体设计的重要作用,指出“总体设计部设计的是系统的‘总体’,是系统的‘总体方案’,是实现整个系统的‘技术途径’。总体设计部一般不承担部件的设计,却是整个系统研制工作中必不可少的技术抓总单位。”

当前,国家信息资源开发利用中,政府电子政务、公益信息服务、信息资源增值利用等开发利用工作取得了良好的社会效益,“十二金”工程部分项目已经达到了良好的预期。中共中央办公厅、国务院办公厅于2004年12月下发了“关于加强信息资源开发利用工作的若干意见”,各省、自治区、直辖市和有关部门正在积极组织本地区、本部门的信息资源开发利用工作,电子政务正在如火如荼地展开。这些工作标志着国家信息资源开发利用已经迈向了新的台阶。经过几十年的努力,军队信息化资源开发工作也取得了一定的成绩,但是还存在诸多问题,如信息资源开发不足,严重滞后与信息基础设施建设;技术标准、总体规划滞后,新的数据烟囱正在形成;缺乏组织协调机制,数据采集融合困难;法规制度缺乏,信息资源开发利用还处在无

序状态;安全保障体系不够健全,信息资源防护能力弱;组织领导体系尚未建立等等,直接影响着军队信息资源开发工作的健康开展。这些问题如果不解决,军队信息资源开发利用就上不了新台阶。但无论问题有多少,核心问题还是总体规划不强。加强军队信息资源规划建设,是当前军队所面临的紧迫任务,只有基于信息资源规划才能较好地制定出总体解决方案,也只有结合信息资源规划,才能使数据标准化工作落到实处,这是实现信息资源开发利用目标的“技术途径”。

信息资源规划包括需求分析和系统建模两个阶段,基本工作步骤和内容大致是:调查分析信息需求和数据流,建立信息系统模型—功能模型、数据模型和信息系统体系结构模型。对信息需求和数据流进行调查分析,要建立和执行用户视图;建立数据模型,要建立和执行数据元素标准、信息分类编码标准和数据库标准,因为作为逻辑数据库的基本表是由标准化的数据元素和信息分类编码组成的。要搞好信息资源规划就必须抛弃传统的信息系统开发模式,学习和掌握系统科学的思想,建立系统工程思维体系,综合运用多种信息技术,特别是信息组织技术,做好信息资源规划,跳出“重硬轻软,重网络轻数据”的误区。因此,结合信息资源规划进行数据标准化建设,树立系统工程的科学方法,是我们解决军事信息资源数据标准化建设的可行途径。

#### 参考文献

- [1] 高复先著.《信息资源规划—信息化建设基础工程》.北京:清华大学出版社,2002年4月
- [2] 高复先.“金字工程—数据标准化的再认识”.《中国信息界》杂志,2004年6月下
- [3] William Durell, DATA ADMINISTRATION—A Practical Guide to Successful Data Management, McGraw Hill, Inc., 1985

#### 作者联系方式

通信地址:通信指挥学院发展战略研究所

邮政编码:430010

联系电话:027-82968233 13397190085



# 基于虚拟现实技术的现代作战模拟系统

梁晓松 许少斌

**摘 要:** 本文从技术和应用两个方面介绍了基于虚拟现实技术的现代作战模拟系统的发展现状,阐述了作战模拟系统在军事变革与新战法研究中所起的重要作用及其广阔的应用前景。

**关键词:** 虚拟现实; 作战模拟; 仿真

## 1 引言

作战模拟是指人们用各种方法对实际作战环境、军事行动和作战过程的描述和模仿,是计算机技术、军事运筹学理论和战役战术学相结合的产物。具有现代意义的作战模拟源于冯·莱茨维兹发明的一种用沙盘、地图、棋子和计算表模拟军队交战过程的器材——兵棋(WARGAME)。它不仅能真实地模拟作战行动,同时能对整个作战过程进行“定量分析”,因此被广泛应用于作战计划的制订和评估中。随着计算机技术的飞速发展及其广泛运用,从20世纪80年代起,美军就开始将计算机模拟技术引入作战模拟试验,将兵棋模拟发展为现代作战模拟,并广泛应用于战斗模拟实验中,拓展了作战模拟的应用范围。运用计算机技术开发的现代作战模拟系统,特别是采用了虚拟现实技术的作战模拟系统,为训练人员提供了一种可以最大限度贴近实战的全新模拟方式,受到各国军队的广泛重视。

## 2 作战模拟技术

海湾战争中,美军利用“军团战斗作战模拟系统”对地面作战的战斗指挥计划进行模拟分析,拟定了俗称“4天计划”或“100小时战争”的作战方案。经“沙漠军刀”行动的实战检验证明,模拟精确地描绘了实战,而实战又忠实地体现了模拟,在模拟基础上制定的作战计划取得了巨大的成功。这一实例再次验证了作战模拟系统在辅助决策、优化方案和军事训练中所起到的重要作用,因此,作战模拟系统被称为“战争实验室”,在这个实验室中进行作战和训练模拟,检验军事理论,训练军事指

挥员和战斗人员,都具有良好的效益。

作战模拟仿真技术,又称为作战虚拟现实技术或作战模拟技术,是实现“战争实验室”的核心技术。该技术以创造逼真的“模拟合成环境”为主旨,集计算机技术、图像生成技术、立体影像技术、传感器技术、信息合成技术、虚拟现实技术等于一体,以作战原则、作战结构为基础,用模拟训练的方法改变训练的过程和形式,提高训练质量和效益。依靠真实战场的数据,利用虚拟现实技术,构成一个具有真实感的虚拟环境,为作战模拟与训练提供一个“可进入”的战场环境仿真平台<sup>[2,3]</sup>,是现代作战模拟与传统作战模拟系统间最大的区别。由于可以建立逼真的战场环境,许多原先无法做到的事情现在都可以在模拟环境中进行,为作战指挥战备训练提供了更直观的感知方式,虚拟现实技术则是构建这种直接感知的现代作战模拟系统的关键。

## 3 虚拟现实技术

虚拟现实(Virtual Reality, VR)技术最显著的特点是交互、想象和沉浸,虚拟现实系统提供了真实感很强的三维场景,以自然友好的方式进行人机交互,使人“沉浸”在场景环境中。虚拟现实技术应用于军事系统中,改变了以往指挥员在沙盘或平面地图上的认知方式,代之以逼真的三维场景,有利于指挥员全面地认知战场,并据此做出正确的判断决策。与网络技术的融合,打破了使用虚拟现实作战模拟系统时的地域限制,通过网络可以实现多个异地分布的模拟系统间的交互,形成了分布式虚拟现实(Distributed Virtual Reality, DVR)系统。

DVR是一个支持多人实时通过网络进行交互

的图形系统。其利用以沉浸、交互和想象为特征的虚拟现实系统,通过计算机图形技术来人工合成按照用户的输入而变化的模拟仿真环境,借助各种传感器实现用户在虚拟环境中身临其境的感受,弥补了现有网络环境中存在的所建构的情境缺乏真实感、交互方式不够友好的不足。为进一步加强交互参与者之间的情感表达和协同群体感知,增加可感知性和自然性,计算机支持的协同工作(Computer Supported Cooperative Work, CSCW)正逐步融入DVR,发展为协同虚拟现实(CVR)。CVR将地域上分散的各个群体借助计算机及其网络技术,实现共同协调与协作来完成同一项任务,通过建立协同工作环境改善人们的信息交流方式,使个体通过网络和计算机技术同群体内的其他个体协同地完成工作,克服了传统协同方式的时空障碍,大大提高群体协同工作的质量和效率。

## 4 虚拟现实技术的军事应用

运用虚拟现实技术实现作战模拟系统中的战场环境仿真,构建多维、可感知、可度量的逼真虚拟战场环境,提高参训者对战场环境的认知效率,更好地辅助指挥员的指挥决策。虚拟现实技术解决了作战模拟系统中真实性的问题,提高了作战模拟的仿真度。分布式网络技术则扩大了作战模拟的规模,使部队足不出户便可参与各种作战模拟行动,为多军种联合训练、盟国的联军训练以及现役与后备役的合练等各种联合作战演练提供了可能性。同时,借助于虚拟现实技术友好的人机交互方式,训练装备操作人员的操作能力,提高作战人员对武器装备的熟练使用度。

目前,虚拟现实技术在军事领域的应用主要集中在以下几个方面。

### (1) 虚拟战场环境

它是指利用虚拟现实技术,通过计算机系统和其他辅助设备对获取或存贮的战场要素数据,比如:战场地形、战场场景、战场态势、战场人员、战场武器装备等进行处理,最终显示出近似逼真的立体战场环境<sup>[3]</sup>。虚拟战场环境能够为计算机作战推演、半实兵演习、实兵演习提供与实际演习区域相同的仿真环境,也可以为特定的训练科目拟构出典型的训练环境(在现实中并不存在),将其作为不同兵种的作战人员共同训练的平台,作战人员通

过各种传感设备与虚拟战场环境相连接,共同感受虚拟战场环境中预先设定的训练内容和预案,并执行相应的作战行动,不同兵种的作战人员通过训练能够达到行动的相互协同。

### (2) 军事训练

虚拟现实技术用于军事训练可实现战斗力的系统集成,并将军事训练推向实战化,既达到使官兵“身临其境”实施训练的目的,又比实兵演练节省大量的人力、物力。因此,在单兵训练、战术训练和诸军(兵)种联合战役训练等课目中都广泛地应用到协同虚拟现实技术。

### (3) 武器装备的研制与开发

将虚拟现实技术应用于武器装备的研制与开发,可以做到在整个武器装备的研制开发过程中边设计边开发,边测试调整边开发,从而缩短了开发时间,节约了开发费用。

## 5 美军分布式作战模拟系统实例

美军对计算机模拟与虚拟现实仿真技术的应用一直走在世界的前列。早在20世纪80年代初,随着军事需求与技术的发展,美军发现各单项武器系统的仿真已不能满足武器装备发展和部队训练的需要。于是,美军开始探索将原已建成的、分散在各地的单武器平台仿真系统或仿真实验室,通过信息互联构成多武器平台的仿真系统,进行各种作战模拟课目的研究。美军具有代表性的分布式作战模拟系统主要有以下几种。

### 5.1 分布式坦克训练模拟系统(SIMNET)

SIMNET是第一个分布式虚拟现实作战模拟系统(如图1),能够提供一个基于网络的集团演习环境,将分散在各地的坦克仿真器用计算机网络连接起来,进行各种复杂作战任务的训练和演习。其将美国本土及欧洲的10个地区的作战环境置于系统之内,可使200辆装甲车辆异地参加统一指挥的可交互模拟演练。每个模拟器以美国的M1主战坦克为单位,提供作战区域内精确的地形起伏、植被、道路、建筑物、桥梁等信息。坦克手可以在模拟器中看到由计算机实时生成的战场环境以及其他战车图像。



(a) 战车模拟器内部



(b) 战车模拟器外壳

图1 “SIMNET”中的坦克模拟驾驶器

## 5.2 战争综合演练场 (Synthetic Theater of War, STOW)

STOW 是一种综合的集成环境,即在一项训练/演习或实验场景中对两个或两个以上的现场、虚拟和推演模拟系统进行综合的基础上而形成的演练环境。1997年10月,美军采用 STOW 系统进行了“统一行动 98-1/STOW”联合演练,共有 3700 多个参演实体,8000 多个参演对象,使用了  $500 \times 750$  平方公里的合成地形环境进行演练。演习中系统达成的目标有:在一个现有的联合合成战场空间中建立新系统模型并对其作战效能做出评估;可以使用世界上任何地区的地形数据库,这些数据库包含气象、天候、夜暗等附加信息;使新的构想、条令、战术可视化,包括二维战场的可视化与三维战场的可视化;人在回路,评估新的  $C^4I$  过程与装备;使用用户友好的事后讲评(AAR)系统,通过试验收集和评价数据等。对 8000 个仿真实体的自如支持,表明作战模拟的系统仿真结构可扩展性达到一个里程碑性的高度。系统实现了与  $C^4I$ 、环境以及基于知识的兵力集成和通用数据基础结构的成功整合,论证了《联合 2010 构想》(目前为联合 2020 构想)在训练、任务重演与发现所要求的使用仿真演练所要达到的低费用与高效率目标。

## 5.3 联合仿真系统 (Joint Simulation System, JSIMS)

该系统是新一代大型联合作战仿真系统的代表,其为分布在世界各地的美军指挥人员、指挥机构、联合部队以及其他联合组织机构提供用来支持军种或联合训练、使命训练、联合演习和职业军事教育、条令拟制、研究战术、制定和评估作战计

划、评估作战态势、定义作战需求的一体化计算机模拟环境,为各兵种的训练和教学提供包括各种任务、各个阶段的逼真联合训练支持。

2002 年美军运用 JSIMS 进行了“千年挑战 2002”联合军事演习。这次演习被认为是美军历史上规模最大的联合军事演习,包括 15000 个目标,600 个作战平台及 400 种弹药,可产生约 60000 仿真实体和 110000 种交互。共有不同军种的 42 个仿真系统,约 90 多个盟员集成为一个大规模复杂的分布式虚拟战场环境。分散在全美 26 个指挥中心和训练基地的各军兵种指挥人员,在同一战争背景、同一战场态势、同一作战想定下同时同步进行了组织指挥大规模联合作战的模拟演练。陆、海、空、天、电和情报作战各单元试图借助模型支持在虚拟的联合作战空间内完成数据交换与信息共享,创造出一个横贯战略、战役、战术三个层次,行动自适应与自同步的、逼真的虚拟战场环境(如图 2)。

分析美军这些现代作战模拟系统及其应用情况可以看出,美军的虚拟现实作战模拟系统已经进入实用化阶段,广泛应用于各军兵种的单兵单装训练、作战指挥训练、战役战术训练、联合作战训练等各个层次。虚拟现实作战模拟系统最大限度地营造出逼真的战场环境,模拟未来战争的各种可能情况,对受训者最大限度地进行贴近实战的锻炼;在逼真战场环境中的这种训练可以反复、节省、安全地执行各类作战行动,增强作战人员的现实战场环境感知意识,使其在实兵实弹行动前已具备相当熟练的作战技能,提高作战人员处理各种危险突发事件的能力。通过虚拟现实作战模拟系统,美军甚至可以超前训练尚未装备的武器系统,验证各种新的作战条令、理论、战法,为应对未来战争提供充

分的实验依据，具备了直接为实战和战争服务的水平，成为提高部队的战斗力的一种经济、高效的新手段。



图2 JSIMS 训练环境

## 6 结束语

与虚拟现实技术、网络技术等现代科学技术的结合，为古老的作战模拟带来了新的生命力。特别是分布式虚拟现实技术的出现，更为作战模拟提供了身临其境的战场环境，扩展了作战模拟的应用领

域，使其不仅在军事训练方面发挥了巨大的优势，也为二十一世纪实现新军事变革及新战法研究提供了良好的虚拟战场环境。基于虚拟现实的作战模拟系统作为新世纪军队建设的重要平台，将在新时期军队现代化建设中发挥越来越重要的作用。

## 参考文献

- [1] 徐学文、王寿云，现代作战模拟，北京：科学出版社，2001
- [2] 游雄，基于虚拟现实技术的战场环境仿真[C]，测绘学报，2002.1
- [3] 高俊，数字化战场的测绘保障，测绘学院报告，2003
- [4] 李思昆，分布式虚拟现实技术发展与挑战，国防科技大学计算机学院
- [5] 周洁萍等，协同虚拟地理环境中多用户交流交互模式及实现，地理与地理信息科学，2005.5
- [6] 王亚等，虚拟现实技术在军事领域的应用及对未来战争的影响，现代防御技术，2005.4
- [7] 金伟新，大型仿真系统，北京：电子工业出版社，2004
- [8] 曾芬芳，虚拟现实技术[M]，上海：上海交通大学出版社，1997

## 作者联系方式

通信地址：郑州解放军信息工程大学测绘学院

邮政编码：450052

联系电话：010-66817301      010-66968427

# 指挥信息系统自主管理技术研究

刘必欣 曹江 张捷

**摘 要:** 指挥信息系统的系统管理能力对于其保障水平和作战效能的发挥具有重要影响。本文就指挥信息系统管理技术的需求作了初步探讨,提出了面向指挥信息系统的自主管理体系结构,并对指挥信息系统管理技术发展和应用提出了若干建议。

**关键词:** 指挥信息系统; 自主管理; 体系结构

## 1 引言

一直以来,指挥信息系统的研制重点关注互联互通能力和具体业务系统建设,对于系统的维护管理、性能优化、故障诊断等“看不见”的方面重视不足。作为服务于军事指挥的 IT 系统,当指挥信息系统由研制阶段转入作战保障阶段时,其系统管理能力和水平将直接影响整个系统作战效能的持续、充分发挥,从而影响整个指挥流程的顺畅与高效。

目前,许多民用领域(如金融、电信、医疗)IT 系统建设的实践表明,随着系统规模的扩大,IT 系统所面临的管理困境越来越突出,系统难以被有效的监控、维护和管理,从而造成其管理成本远大于构建成本。以富士公司数据中心为例,其统计数据Display,每投入 1 美元购买存储资源就需要花费 9 美元进行维护和管理<sup>[1]</sup>。系统管理能力与水平已成为制约 IT 系统生存发展和发挥效益的瓶颈。

因此,从提高我军指挥信息系统管理维护水平,充分发挥指挥信息系统的作战效能的高度认识指挥信息系统的管理能力需求,研究面向现代指挥信息系统特点的系统管理技术,构建完整、有效、先进的管理技术体系已成为我军指挥信息系统进一步发展的当务之急。

## 2 指挥信息系统的系统管理能力现状

### 2.1 指挥信息系统管理面临的挑战

我军指挥信息系统的建设随着覆盖领域日益广泛,信息获取手段日益丰富,其系统组成和交互依赖都渐趋复杂。与此同时,对指挥信息系统基础设

施和各类业务系统进行配置、监控、优化、诊断的复杂性也随之提高。

**复杂的系统配置任务:** 安装、配置大型的指挥信息系统是一项非常复杂的工作,即便是受过正规训练的专业技术人员亦未必能轻易完成。美海军陆战队测算,熟练的工程师配置一套电子邮件系统需要 3 天时间。研制试验工作的实践表明,大部分信息传输系统的安装调试通常需要耗费数天时间。

**复杂的系统监控任务:** 高级指挥机构的信息系统通常要支撑数百、甚至数千人协同工作,美军在伊战时,中央司令部工作员超过了三千人,数百台服务器和上千台客户机,分布在不同的指挥位置甚至相隔数千公里,运行着几百个各类组件构成的数千种业务系统。准确地把握系统中各类软硬件资源的状态、精确地记录操作人员的关键操作是对信息系统进行有效维护和监管的必要条件。

**复杂的系统优化任务:** 在瞬息万变的战场环境下,指挥信息系统应能随着业务量的变化不断地调整优化。系统优化是一个涉及从底层硬件资源到上层应用资源的综合工程,然而复杂的决策过程和繁琐的技术参数使得调优工作通常被简单的增加硬件配置所取代。

**复杂的系统诊断任务:** 大型指挥信息系统出现应用故障时,定位问题的位置、分析故障的原因、采取适当的措施进行恢复是个非常耗时的任务,因为系统中所包含的大量网络、硬件、软件资源所形成的复杂依赖关系有时非常隐蔽,除了通晓全盘的专家,一般维护人员很难在短时间里从故障现象中判断出问题根源并找到解决方法。

### 2.2 当前指挥信息系统管理能力的不足

目前,我军指挥信息系统在建设过程中出于朴

素的技术理念在研制中考虑了一定的系统管理要求，具备初步的系统管理功能，例如远程部署及主机状态监控。但总体来说系统的管理能力相对滞后于业务能力建设，难以满足大规模指挥信息系统日常维护和作战保障的需要。主要体现在三方面：在系统管理的功能上，仅少数基础软件和应用系统具有简单的监控统计功能，缺乏完整的系统运行状态感知、探查、控制和动态调整的能力；在管理手段上，信息的收集、理解和处置主要依靠人工干预，缺乏常规管理行为的自动化、智能化手段；在管理水平上，系统管理功能的规划建设主要从单个软件角度考虑，还处于各自为政、自建自管的状态，没有形成系统的、全面的、有效的管理体系。

为此，迫切需要认识当前指挥信息系统在管理能力方面的不足，站在指挥信息系统总体的高度，采用先进的系统管理技术，改造提升指挥信息系统的整体管理能力。

### 3 面向指挥信息系统的自主管理技术

#### 3.1 信息系统管理过程闭环

从过程的观点看，完整的系统管理活动是由事件感知、推理分析、调整干预三个阶段所构成的闭环，如下图所示。事件感知是指定义、触发、传递、汇集与管理目标相关的系统状态和重要事件的行为；推理分析是在感知事件的基础上，运用相关知识和规则得出处置方法的过程；调整干预则是通过调节系统的组织结构、资源配置、组件状态等动作执行系统管理行为，达到系统管理目标。



图1 系统管理过程闭环

在传统的信息系统管理方式中，人，即系统的维护保障人员，是上述管理闭环中必不可少的要

素。包括：部分事件感知任务、大部分调整干预任务和几乎全部的推理分析任务都依赖于手工完成。系统管理的“人治”带来的后果是，系统的维护保障能力很大程度上依赖于维护管理人员的技术素质和规范化程度，从而造成管理水平不稳定，加大了指挥信息系统的维护保障难度。

因此，要从根本上提高指挥信息系统的管理维护水平，必须弱化人在管理闭环中的依赖性地位，提高指挥信息系统在事件感知、推理分析以及调整干预各环节的自动化水平，增强系统自我管理、自维护的能力。

#### 3.2 自主计算

“自主（Autonomic）”一词源于人体的自主神经系统。自主神经在人不知觉的情况下协调人体各个器官，管控心跳、体温、血糖等基本生命体征，维持人体的正常生理机能。将自主概念与信息系统领域相结合源于 IBM 公司提出的“自主计算（Autonomic Computing）”概念<sup>[2]</sup>，其主旨是通过在系统中建立有效的、多方面的自我管理能力来降低系统的管理成本，提高系统的管理效能，从而满足动态环境下复杂系统的管理目标。“自主计算”概念提出后在 IT 界得到迅速认同和推广，包括 Oracle、Sun、HP 等在内的主要 IT 厂商均将其纳入关键技术体系。

结合我军指挥信息系统的实际，我们认为，自主计算的理念为展开指挥信息系统管理技术体系的研究提供了一个很好的理论基础和目标蓝图。将自主计算的原理和技术运用于指挥信息系统，着力增强其自我管理、自维护能力，对于提高我军指挥信息系统管理维护水平具有重要意义。

#### 3.3 指挥信息系统自主管理体系结构

基于自主计算的原理，我们开展了面向指挥信息的自主管理软件框架，提出面向指挥信息系统的自主管理体系结构，如图 2 所示。

在指挥信息系统自主计算体系结构中，指挥信息系统的系统管理剖面由三个层次构成，由下到上分别是执行层、汇集层和决策层。如果把整个体系结构比作人体，那么执行层是自主管理体系结构的“四肢”，决策层是“大脑”，汇集层则是“神经”。

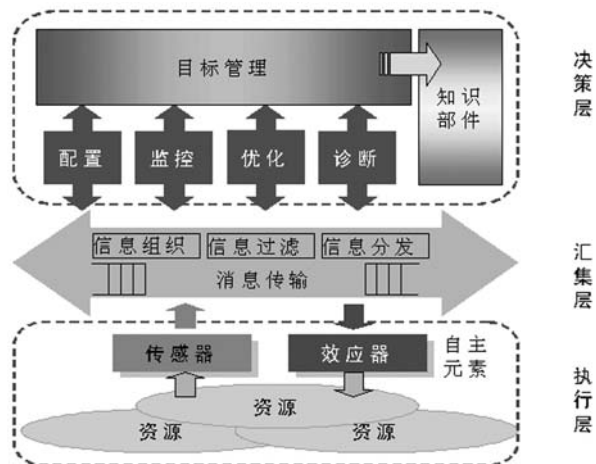


图2 面向指挥信息系统的自主管理体系结构

作为整个管理体系的末端，执行层可抽象为若干自主元素所构成的集合。所谓自主元素是指具有自我感知和行为调整能力的管理单元，由被管资源和资源代理构成。被管资源具有广泛的意义，不仅包括计算资源（如 CPU、内存），还包括构成指挥信息系统的网络资源（如带宽）和软件资源（如缓冲区、请求队列、连接数、线程池等）。资源代理是对被管资源的标准化封装，它在各类不同特质的资源之上提供标准化的资源界面，使得之具有一致的信息感知接口和行为调整接口，这是自主管理的基础。资源代理可分解为传感器和效应器两个主要部分，前者主要依据特定的模式探查资源的属性和状态，传递给管理决策层，后者依据管理决策，执行资源的行为调整动作，从而完成系统管理功能。

汇集层的主要功能是完成管理信息和管理决策的“上传下达”，是决策层与执行层之间的消息总线。汇集层不仅提供基本的消息传输能力，更为重要的是支持管理信息的组织、过滤和多种分发模式，使得执行层的零散事件形成有机联系的信息报告到决策层，并将决策层的指令高效准确地分发到执行单元。

作为自主管理体系结构的中枢，决策层的主要作用是驱动管理信息收集、进行管理信息的分析推理、并产生管理指令。我们使用“目标”来刻画自主管理器的功能刻画，例如为指挥信息系统设置配置、监控、优化和诊断四个目标，并通过相应的管理任务实现。决策层的核心是用于知识管理和推理分析的知识部件，它基于相应的管理知识库，通过对管理目标进行分析、分解和冲突消解，产生具体的管理任务。例如，对于系统优化目标，知识部件

将加载“优化任务”，订阅或轮询一组自主元素（如队列中请求数），并设置事件响应规则（如，“若等待队列中请求数已超过 20 将线程池容量增加一倍”）；当对应事件后，知识部件触发相应的处理逻辑，将调整指令传递给相应自主元素的效应器来实现优化。

在自主管理体系结构中，指挥信息系统中的各自主元素在决策层的指挥下、在汇集层的协调下，构成具有特定组织结构、自我感知力、自我调整能力的自治系统。指挥信息系统自主体系结构为开展指挥信息系统管理技术研究和系统研制提供了一个可供参考的技术框架。

## 4 推进指挥信息系统管理技术发展和应用的设想

指挥信息系统的快速发展和推广应用对我军信息管理系统管理技术发展提出了迫切需求，也为我军信息管理系统管理技术发展提供了良好的契机。下面笔者就推进指挥信息系统管理技术发展和应用提几点初浅建议。

第一，转变观念，重视管理需求研究。

首先需要改变以往系统研制过程中重业务功能、轻管理手段的观念，充分认识管理水平对于指挥信息系统进一步发展的重要意义，加强信息管理系统管理基础理论研究，并在组织运用实践中总结归纳管理维护手段需求，形成既贴近实战又具有一定前瞻性的指挥信息管理系统管理需求理论。

第二，统筹规划，加强系统顶层设计。

系统管理能力是信息系统能力构成不可分割的一部分，既与指挥信息系统的各业务功能要素存在紧密的横向联系，又在纵向上构成一个相对独立的管理要素体系。又这一特点要求指挥信息管理系统管理能力建设一方面要与业务能力建设统筹考虑、同步发展，另一方面又必需作为一个整体性系统进行充分的总体论证和顶层设计，从技术体制和规范标准上统一全军指挥信息系统的管理技术状态，从而改变当前指挥信息管理系统能力不健全、不完备、不均衡、不实用的状况。

第三，先“破”后“立”，逐步推进现有系统改造。

事件和状态感知是进行系统管理的前提，这首先要求打破指挥信息系统目前的“黑箱”状态，综

合运用反射技术、消息中间件技术、知识表示与智能推理技术，建立标准、一致的事件感知接口和调整干预接口，在统一的技术体制成体系地研制系统管理基础设施和功能插件，与现有基础设施和业务系统集成，逐步丰富上层管理应用，变“管不了”为“管得好”，在滚动发展中推动指挥信息系统走向成熟。

第四，立足实效，注意把握人机平衡。

系统管理活动的自动化智能化是自主管理的目标，但一味地追求高智能化可能脱离部队运用实际，增大建设成本和应用风险，因此系统管理能力建设应与部队维护保障的实际紧密结合，立足常规管理活动的自动化，注意把握好自动处置与人工干预之间的关系，做到既符合需要，又经济高效。

## 5 结论

指挥信息系统是未来信息作战的“神经”，对获得战争优势具有举足轻重的作用。在全军指挥信息系统建设迈上一个新台阶的今天，加强系统的管理能力建设既是指挥信息系统走向成熟的需要，更是提高其维护保障水平、充分发挥其作战效能的需要。本文就指挥信息系统管理技术的需求做了初步探讨，提出了面向指挥信息系统的自主管理体系结构，并对指挥信息系统管理技术发展和应用提出几点不成熟的建议，仅供大家参考。

## 参考文献

- [1] K. Evans-Correia, “Simplifying Storage Management Starts with More Efficient System Utilization,” Interview with N. Tabellion, searchStorage (August 29, 2001)
- [2] IBM, Autonomic Computing: IBM’s Perspective on the State of Information Technology, 2001

## 作者联系方式

通信地址：北京市丰台区大成路 13 号 R02

邮政编码：100039

联系电话：010-66820295-820 13621262576



# 图书馆特色数据库建设的理论与实践

刘迎风 曾纲京

**摘 要：**以本馆特色数据库建设为例，介绍了特色数据库建设的设计目标、建库原则、实施方案及主要内容，阐述了特色数据库建设的理论意义与实践效果。

**关键词：**数字图书馆；特色数据库；信息资源数字化

图书馆作为学院文献信息中心和动态发展的信息资源系统，是加强院校教育信息化、现代化建设的重要阵地，是学院培养高素质人才的重要场所，是学院建设发展的重要组成部分。数字图书馆的研究和建设，给图书馆事业带来了一场革命，改变了传统的知识传播方式。根据形势的发展和军队院校教学改革的需要，总部要求全军院校图书馆以“科技兴馆”为发展战略，以数字化建设为发展方向，逐步实现信息传输网络化、信息资源数字化、信息利用共享化、信息管理有序化，为军队院校教育信息化建设服务，为培养高素质新型军事人才服务。

## 1 设计目标

图书馆特色数据库建设的总体目标是资源丰富、先进实用、功能完善、易于扩充、操作方便、可维护性好，以资源共享为目的，建立起能够及时反映本院学术水平的共享型网络数据库，集多种信息于一体，提供多种检索途径，为网上用户提供浏览、查询、导航、全文检索等服务，为学院的教学、科研和管理提供快速、全面、准确、优质的数字化文献信息服务。

## 2 建库原则

### （1）计划性与经济性原则

数据库建设要进行整体规划，采取合理布局、重点投入、分步实施、从易到难、讲究实效等措施，使数据库尽早投入实施运行阶段。依托图书馆现有局域网络，再购置先进的服务器、NAS、计算机终端、高速扫描仪等设备，节约不必要的开支。

### （2）先进性与标准化原则

数据库建设的硬件设施选用先进的设备，软件选用全军院校最新推广应用的《军队院校数字图书馆应用软件系统》（MDLS），确保软硬件系统的先进性，以适应未来发展的需要。数据库建设符合军队院校建设标准，便于今后实现资源共享

### （3）完备性与可扩充性原则

数据库所收录的数据要保证本专题门类的完整性，建成的数据库应支持开放式的体系结构，以便于未来的扩充、升级和换代。

### （4）可靠性与安全性原则

数据库应具有充分的安全和保密措施，要设置多级安全管理，加强人员管理与数据管理。上网发布前经过学院保密委员会审察，慎重给予用户权限。

## 3 实施方案

数据库建设分为三个阶段：第一阶段为筹备和启动阶段，即为前期准备工作，主要完成数据库的总体结构框图，按照边建设边服务的方针，以系统形成最初的服务能力为主要标志；第二阶段为数据库全面建设阶段，初步完成系统建设的总目标，以数据库开始发挥显著效益为主要标志，第三阶段为数据库进一步优化、完善和维护阶段，以全面实现数据库建设总目标。

## 4 主要内容

陆军航空兵学院图书馆作为《军队院校数字图书馆应用软件系统》（MDLS）的首批试用单位之一，对该系统的应用十分重视，利用该系统建成系列特色数据库，包括“直升机与发动机工程学术论

文”、“陆军航空兵学院学术论文”、“陆军航空兵学院学报论文”等三个全文数据库。

#### (1) 软硬件平台的构建

数据库建设依托图书馆现有局域网络,硬件设施主要有服务器、NAS、计算机终端、高速扫描仪等设备,备份设备选用磁带机1台,另外配备高速扫描仪2台,工作计算机终端若干台。

建库软件选用全军院校最新推广应用的《军队院校数字图书馆应用软件系统》(MDLS)1.0,服务器操作系统选用 windows server 2003 iis6.0,客户端操作系统选用 windows 2000 server/professional 与 windows xp。

#### (2) 数据收集整理

数据收集是数据库质量的重要保证,因此,必须紧密围绕专业特色这一主题,数据的采集坚持学术性、资料性、准确性、实用性、系统性和价值性,保证数据全面、质量可靠。

#### (3) 数据库结构设计

在熟练掌握《军队院校数字图书馆应用软件系统》(MDLS)建库功能模块的基础上,结合不同数据库的特点,设计库结构:确定分类导航体系,参照数据资源分类规范,设置导航树;确定著录、检索、概览、细览等字段;设定用户级别及权限;设置编目模板;确定著录深度、发布界面等。

#### (4) 建库人员培训

建库人员的水平也是影响数据库质量的关键因素,我馆先后派两名技术人员参加了《军队院校数字图书馆应用软件系统》培训班。在掌握了该软件系统的使用后,组织馆内人员开展建库工作,按扫描、识别、格式转换、电子书加工、分类标引、主题标引等工作流程建立起专门的队伍,同时与学院2110重点学科专业教员合作,由图书馆提供软硬件平台、负责技术培训和分类标引,并与该专业的专家、博士等人一起按学科特点,建立分类导航体系,确定标引深度等。

#### (5) 数据加工与发布

数据加工与发布是建设数据库的主体工作,包

括数据筛选、标引、编目、录入等工作。收集到的数据入库前,一定要进行认真的审核筛选,去掉重复的、不准确的,最终确定哪些数据被收录进数据库。标引结果的好坏影响数据库的质量,决定数据库的检索效率。因此,应根据实际情况,选择合适的标引方式、制订标引细则,具体规定标引的深度、分类的集中与分散、主题词和关键词的选用规则等,提高标引质量。数据录入也是不可忽视的重要环节,为了确保输入数据准确无误,要制定严格的质量管理制度。

首先进行数据准备,将各种类型的文档按篇保存,并转换成数据库需要的格式,再由从事编目的专业人员为数据库中的论文分类,给定中图分类号,并使用《数字资源元数据 MDC 著录手册》,查阅字段信息,为数据库论文编目,进行元数据加工,再按《数字资源分类规范》,引入相应类别,最后进行数据发布。

#### (6) 数据库审校与维护

为避免标引错误,提高标引的一致性,减少数据录入中的失误,保证每一条记录的准确性,要全面、认真、细致地做好审校工作。对发布后的数据库进行网上点击、浏览,检查、校对数据的准确性、完整性,发现问题及时修改,并备份数据,采用边建设边备份的方式,确保数据的安全性。

数据库建成后并不意味着大功告成,还要进行经常性的更新和维护,才能保持生命力。要收集数据在使用过程中的反馈信息,及时对数据进行替换、删除、修改和整理。在数据库初步建成后,对数据库随时进行更新维护,及时追加新产生的数据。

## 5 效果

图书馆特色数据库的建成提高了我馆的信息保障能力,为学院的教育信息化、现代化提供了较好的信息保障,为教员、学员提供方便使用的网上教学参考资料,提高教学质量,发挥重要作用。

#### 参考文献(略)

#### 作者联系方式

通信地址:陆军航空兵学院训练部图书馆

邮政编码:101123

联系电话:010-66877627 13161287257

# 军队信息资源共享的原则与思路

罗永健 杨鑫 郭强 郭诗军

**摘 要:** 随着我军信息资源开发利用工作的进一步深入,信息资源共享的地位与作用正变得越来越重要,已成为军队信息化建设的关键。本文从我军信息资源开发利用的实践出发,首先根据信息资源的特点分析并指出了军队信息资源共享应遵从的六项原则,在此基础上从管理体制、政策法规、保障机制、技术支撑几个方面详细阐述了军队信息资源共享的实现思路,为建立我军信息资源共享的长效机制提供了有益参考。

**关键词:** 信息资源共享; 原则; 思路; 军队信息化建设

信息资源共享是军队信息资源开发利用的目标,也是信息化建设中极其重要的内容。通过多年来的建设,军队信息资源开发利用按照“打基础、抓应用、谋发展”的思路,整体规划,稳步实施,取得了显著成绩。但我军的信息化建设起步较晚,总体上仍处在初步阶段,发展很不平衡,尤其是信息资源共享缺乏统一规划和管理,标准不一、重复建设、纵强横弱、互通互操作难等问题日益突出,形成了许多大小“烟囱式”的信息孤岛,严重影响了信息资源在军队各个部门、战争各个要素间的有效流动和共享,成为现阶段军队信息化建设亟待解决的问题。因此,必须加大对军队信息资源共享的理论和实践研究,充分发挥整体信息优势,尽快提高信息资源开发利用的工作效益,推动军队信息化建设的又好又快发展。

## 1 军队信息资源共享的原则

军事信息资源一般具有如下的特点:一是层次结构纵横交错、信息密级不一;二是服务应用种类繁多、流程复杂、涉及的职能部门众多。因此军队信息资源共享是一个复杂的过程,共享内容广泛,必须遵从一定的原则才能保障信息资源共享的有效实施。

1) 需求牵引原则。要调查和分析军队跨部门(系统)应用的业务流程,梳理各部门(系统)间信息交换与共享的需求,并把这种需求作为信息资源共享建设的动力和方向,在此基础上构建起信息交换、共享的框架和平台,以满足业务需求作为信息共享各项建设的出发点和归宿。

2) 制度化原则。要把军队部门(系统)信息交换、共享制度化,把为其他部门(系统)提供有关信息列入部门(系统)的职责范围,努力促使把交换、共享信息资源作为制度约束下的一种自觉行为。制度保畅通,只有在制度化原则下才能有效推动部队整体的信息交换和共享能力。

3) 分工与合作原则。信息资源共享是一项涉及到方方面面的系统工程,必须从全局角度上进行统一安排。所以要建立基础信息资源、专业信息资源的分工合作原则,各部门、单位相互配合,共建共享,避免不必要的重复和浪费,从而发挥出整体效益。

4) 标准化原则。标准的问题一直是军队信息化建设的一个重要问题,也同样是信息资源共享的一个核心问题。要建立信息资源的采集、加工、存储、交换、发布标准规范,并在统一的标准下确立军队信息资源共享的有效机制,来满足信息共享的技术要求。

5) 安全保密原则。军队是一个特殊性团体,具有严密的组织性和保密性,其组织功能和作战功能的发挥,一方面要求高度的信息共享,另一方面又要求分层次、有权限的实施安全共享。因此要建立权限管理制度,把信息安全技术和信息安全策略贯穿于信息资源共享的全过程。

6) 集成共享原则。军事信息系统中异构型数据库大量存在的现状决定了现阶段的信息共享必须依赖于系统的综合集成。集成是把不同来源、格式、特点性质的数据在逻辑上或物理上有机地集中,提高数据的完整性、准确性和一致性,确保数据在应用中按需流动和交换,从而为用户提供全面

的信息共享。

按照上述原则,要站在军队建设全局的高度,结合当前信息资源共享过程中出现的各种问题,积极探索军队信息资源共享的长效机制。要形成军队信息资源共享的完整思路,通过不断完善信息资源共享的管理体制、政策法规、保障机制和支撑技术等方面,充分利用行政、计划和预算等手段,协调部门之间信息的共享,强制推动军事信息在相关部门间的交流,避免各单位信息封锁、难以互通的现象发生,根除“信息孤岛”现象。

## 2 军队信息资源共享的管理体制

面对新军事变革和对信息资源共享的需求不断扩大的挑战,我军应改革机械化、半机械化军队形态下旧的管理体制,建立健全适应军队信息化建设和满足信息资源有效共享的新的管理体制。

### 2.1 军队信息资源共享的两种主要管理方式

1) 集中式管理。集中式管理是由组织系统的高层管理者统一制定规划计划、资源分配和组织实施的管理。实行集中管理是军队管理的重要原则,也是军队信息资源共享的重要特性和基本要求。

在新的历史条件下,资源的相对有限和军队现代化建设、军事斗争准备高投入、高消耗、高风险的特点,要求对人、财、物、时间和信息等资源实行集中管理。因此,应注重改变领导体制的分散和多层次,实现由分散管理体制向集中管理体制的转变。这就要求搞好顶层设计和整体筹划,抓紧制定信息资源共享的管理条例和技术标准,努力实现上下左右的互联互通互操作,达成信息资源的充分共享。

2) 扁平式管理。信息资源共享的一个重要特征就是要求信息传递快,只有及时传递的信息才具有共享的意义,因而实现信息资源的共享要求建立适合信息快速流动的扁平网状管理体制。

扁平网状管理体制的特点是,外形扁平,横向联通,纵横一体,能加快信息的流动速度,提高管理的灵敏性。外形扁平就是尽量减少管理层次,缩短信息流程,使尽量多的管理单元同处于一个信息流动层次;横向联通就是各平级单位之间直接沟通联系,各平台之间能实时交换信息;纵横一体就是

整个系统实现信息采集、传递、处理、存储、使用一体化。

### 2.2 军队信息资源共享的组织体制

军队信息资源的共享,应纳入全军统一规划和管理,由专门机构来具体负责实施。统筹兼顾,统一规划,从全局出发,重点规划设计不同部门协同工作的内容和流程,打破信息资源“部门割据”、“条块分割”的局面,解决军队信息资源为各个部门所有、各个部门垄断的问题,真正实现信息资源的交流与共享。

美军在新时期所建立起来的首席信息官制度对加强我军信息化建设、完善高层领导协调体制有重要的参考作用。2003年编制体制调整时,我军确定成立全军信息化领导小组、办公室和专家咨询委员会,这是我军体制编制调整的一个“亮点”,为我军信息化建设提供了组织保障。随着信息化建设的进一步深入和信息共享需求的进一步增加,还应强化各级信息资源共享组织机构的职能,来加强对跨领域、跨部门间信息资源共享的协调和沟通。

### 2.3 军队信息资源共享的业务体制

军队各级、各类信息资源共享管理机构接受同级以上信息共享管理部门的业务领导。各个信息共享管理部门通过信息网络互联互通,建立业务协作关系,实现部门间的信息资源交换与共享。

军队信息资源共享按规划实行集中与分布式相结合的方式建设。基础性的数据库集中建设,各部门共享;专业业务性的数据库分布式建设,各部门按需要有条件共享。基础数据采集由业务主管部门一家采集提供各部门共享,保证数据源头单一性及数据的准确性。

## 3 军队信息资源共享的政策法规

军队信息资源共享是目的性、组织性很强的一项系统性复杂工作,为了保证这一工作的有序和高效进行,需要制定一系列有关军队信息资源共享的方案、制度、规定、条例等,明确各相关主体的责任、权利和义务,为军队信息资源共享提供一个良好的法律政策环境。

### 3.1 军队信息资源的共享服务政策

共享服务就是使信息能够便捷地、按照一定要求的被用户无障碍地获取。共享服务政策的主要内容有:

1) 军队信息资源公开政策。信息公开是实现军队各部门之间信息共享的必要条件和基本前提。需要对军队信息资源进行总体梳理和规划,界定军队保密信息、内部共享信息、公共信息的范畴,根据信息的不同性质制定不同的公开与保密级别,凡不属于保密的都应列在公开的范畴。

2) 军队信息资源采集政策。军队信息资源共享对于采集政策提出的要求是确保业务部门间的相互协作,避免重复采集,提高共享数据质量。

3) 军队信息保障政策,包括军队、各系统各部门的信息共享指导政策、军队信息共享基础设施建设政策、人才保障政策、机构管理政策等。

4) 军队信息交流与合作政策,包括标准统一指导政策、跨系统与部门的信息交流与合作政策等。

### 3.2 军队信息资源共享的经费投入政策

为进一步推动信息化建设与规范、加强信息资源共享,推动共享体系的建设,军队要为信息资源的共享建设加大资金投入,并制定相应的资金投入和管理政策。对投入的经费要统筹安排,公共部分的建设要设立专项经费予以保障,对各单位资金分配要合理有度。在资金投入过程中,要切实加强资金管理,完善资金管理制度和资金使用的绩效考评制度,提高资金使用的规范性和有效性。

### 3.3 军队信息资源共享的保密制度

安全保密是信息资源共享的首要保证。缺乏有效的安全手段作保障,信息资源就不可能发挥效益,甚至是反面效益。因此,要积极制定军队信息资源共享的安全保密制度。

### 3.4 军队信息资源共享的管理政策

军队信息资源共享的运行需要有效的管理,需要制定科学的管理政策。管理政策涉及的内容很多,其中如何实现管理体制的创新是军队信息资源共享政策体系建设首先要解决的问题。

另外,要营造共享的整体氛围,为军队信息资源共享政策的制定和实施创造有利条件。同时必要时还需要强制性手段,来保证全军信息资源的有效共享和整体作战效能的提高。

## 4 军队信息资源共享的保障机制

军队信息资源共享是一个长期的建设过程,如何确保其稳定、持续、有力地得到执行,防止成为束之高阁的“摆设”,是我军当前信息化建设中急需解决的问题。

### 4.1 军队信息资源共享的人才保障机制

目前,实现全军范围的信息资源充分共享,一个突出问题就是“重硬轻软”,而人的素质又是“软件”里的一个核心要素。因此,一方面要充分发挥院校、科研所在信息资源理论研究方面的优势,大力培养信息资源管理理论研究的队伍和人才,推动信息资源管理思想的普及;另一方面要充分发挥各类培训基地、信息中心的职能、专业作用,利用其人力、远程、多媒体和电脑教室等软硬件资源,加强对广大干部、士官特别是主管信息化工作的各级领导干部信息共享知识和操作技能的培训、网络环境下的工作方法和能力的培训。

此外,还要通过广播、电视、报刊、网络等多种形式,加大对计算机和网络知识、信息资源建设、共享知识的普及教育,努力提高全军信息化的思想认识水平和整体的信息素质。

### 4.2 军队信息资源共享的安全保障机制

影响军事信息安全的因素有很多,如网上黑客入侵、网上病毒泛滥和蔓延,信息间谍的潜和窃密,网络恐怖集团的攻击和破坏,内部人员的违规和违法操作,网络系统的脆弱和瘫痪,信息安全产品的失控等。因此,保障军事信息资源共享,首先要保障共享信息的安全,信息安全是军队信息资源共享中最关键、最根本的问题。

为此,要切实做好军队信息资源的保密管理和安全管理工作,采取切实有效的措施,对信息进行分级管理和访问权限控制,防止信息泄漏和人为破坏。要加强安全技术的研发,并积极采用先进、实用的安全技术、安全产品。同时要建立健全安全规

章制度，加强对人员、组织和流程的管理，科学合理地划分信息保密等级，做好信息共享安全的监督管理工作。

### 4.3 军队信息资源共享的监督和激励机制

为了保障信息资源共享的良性发展，需要建立信息共享的监督和激励机制，根据责任制对部门和主要责任人进行考核，对各部门信息共享的情况进行监督和激励。

#### 4.3.1 军队信息资源共享的监督机制

要对信息资源共享建设以及各部门信息共享的情况进行监督，监督中应注意理顺工作机制，做到主官对所属部门信息共享情况的清楚掌握，同时要让广大官兵参与到监督中来。

1) 必须加强对军队信息资源共享法规的学习和宣传教育，使广大官兵在知法、懂法、用法的基础上，牢固树立依法监督的意识；

2) 要强化监督，通过建立健全监督机制，把业务部门监督与群众监督结合起来、日常监督与定期检查结合起来，形成环环相扣、上下互动的监督机制；

3) 向监督要效益，形成全方位、全过程的共享监督网络。

#### 4.3.2 军队信息资源共享的激励机制

当前，我军的信息化建设任务十分艰巨，在信息资源共享的建设中还存在种种困难，应建立完善的激励机制来激发广大官兵信息资源共享的热情。

1) 需要建立目标激励机制，帮助官兵明确信息化建设为信息共享服务的奋斗方向；

2) 要建立竞争激励机制，在营造你追我赶的氛围中增强信息共享的意识和共享能力；

3) 同时还要建立评估激励机制，把广大官兵在信息共享中所做贡献的准确评估作为业绩考核的主要指标。要通过评估活动，进一步激发广大官兵和各级业务部门、组织坚持信息资源共享的长效机制的积极性。

## 5 军队信息资源共享的技术支撑

1) 构建信息共享互联互通平台。信息共享互联互通平台应由流程管理系统、应用集成系统、应用适配器系统、管理和监控系统、安全支撑系统 5 个基本系统组成。其中，流程管理系统、应用集成系统、应用适配器系统是平台的核心。

2) 全面推行标准化。标准化是实现军队信息资源共享的先决条件。目前，在信息共享方面的相关标准很多，仅国标就达 800 多个，此外还有数目众多的军标。但是如此众多的标准缺乏统一性，标准过多、过泛给信息共享建设带来了很多不便，甚至形成了大量的信息孤岛。因此，要加强标准化建设的管理工作，统一网络和信息的标准规范，统一标准是互联互通、信息共享、业务协同的基础。

3) 加强共享数据库建设。目前，我军信息资源开发和共享相对滞后的矛盾十分突出，在信息化建设中出现了“有路无车”和“有车无货”等现象，许多数据库更新不及时，甚至是“死库”，一些军事信息关键业务不能实现互连互通和互操作。从而造成了许多信息基础设施和技术设备得不到充分利用，制约了信息资源共享的发挥。因此，必须改变目前建库力量分散，低水平重复建设的局面。按照整合、共享、完善、提高的要求，建立军队信息共享数据库，有效调控增量资源，激活存量资源，最大限度发挥现有资源的潜能。

参考文献（略）

作者联系方式

通信地址：陕西省西安市长安区西安通信学院二系通信新技术研究室

邮政编码：710106

联系电话：029-84706542

# 一种全新的国防项目管理信息化服务平台研究

苗苗 孙冲

**摘 要:** 新兴的信息化技术为项目管理提供了新的手段, 国内外的项目管理信息化技术与相关的服务发展非常迅速。论文研究了现有的项目管理信息化服务平台, 在此基础上提出了适用于我国国防项目管理的全新信息化服务平台, 并对该平台的结构和主要功能进行了研究, 最后对该平台的实现及可能面临的问题进行了展望。

**关键词:** 国防项目管理; 信息化; 服务平台

## 1 引言

新兴的信息化技术为工程项目管理提供了新的手段, 运用信息技术促进工程项目管理的优化升级是项目管理领域的一个新兴研究热点。传统的单靠人工管理或单机的管理方式, 不仅信息传递速度比较慢, 而且管理的手段也比较单一, 容易造成工程中资金、人力、质量、进度等方面的失控。因此传统的管理方式已经不能满足项目管理的需求。

借助有效的信息技术, 可以将项目管理中的有关内容有机的结合在一起。目前常用的 MIS、ERP、客户关系管理(CRM)等系统都可用于对组织内部的项目进行有效管理。而 Primavera Project Planner(P3)、MS-Project 以及梦龙公司的“通用项目管理软件”等系列的专业软件, 则更进一步的将 MIS 和价值工程、系统工程与仿真技术等相结合, 可用于排定网络计划、网络计划优化和进度跟踪等, 并具有一定的网络信息交互功能。近年来国内的很多软件公司也开发了一些项目的信息技术产品软件, 然而这些信息技术产品主要的服务对象是企业 and 项目组织, 并没有考虑将业主作为服务对象之一; 而且这些软件的集成能力和通用性都存在不足, 信息标准不统一, 设计不规范, 无法共享等问题, 这已经成为我国推进项目管理的信息化建设的一个瓶颈。

而我军的项目信息化管理相对于商业领域的信息化管理还比较落后, 目前为止还没有较为通用的国防项目管理信息化服务平台出现, 绝大多数的国防项目仍然是依靠传统的人工管理或单机的管理方式, 这样对于大型复杂项目的管理就显得力不从心, 容易造成项目进度、费用和质量失控。另一

方面, 国防项目中的项目甲方(军队和军队的采办管理机构)对于项目成败具有重大的责任, 因而在国防项目中甲方和乙方(承研、承制单位)之间的信息传递非常重要, 在执行项目过程中文档的往来也很频繁。而目前的情况是某些领域的军品研制项目合同管理单位往往同时管理几十个甚至几百个采办项目, 而且不同项目的乙方分布于全国各地, 在采用人工管理和传统通讯手段的情况下很难面面俱到地兼顾所有项目, 在立项审查、审核项目进展、定型管理等方面都难以及时地传递信息和处理问题, 这些都大大制约了国防项目管理领域的发展。

因此, 随着我军信息化水平的不断发展, 国防领域的项目管理也亟待加强, 这就需加强信息化项目的建设, 开发出满足军队需要的新型国防项目管理信息化服务平台。

## 2 项目管理信息化服务平台的现状研究

目前, 项目管理信息化在具体工程项目中的实施主要有三种模式: 第一种是直接购买已有的商业化项目管理软件产品, 适当进行二次开发, 然后安装在企业内部的服务器上, 供项目参与各方共同使用; 第二种是聘请咨询公司或软件公司针对项目的特点自行开发, 并完全承担系统的设计、开发和维护工作; 第三种就是租用服务模式, 即 PM-ASP (Project Management Application Service Provider), 也是本文将重点研究并借鉴的一种信息化模式。

PM-ASP 模式是由专业的 PM-ASP 服务供应商开发出一种项目管理信息化系统, 通过 Internet 提

供给项目组织或者企业相应的信息化服务,通常按照租用时间、项目数、用户数、数据占用空间大小收费。这种服务方式的优点在于其实施的费用最低,使用的方式灵活,而且维护的工作量不大。在国外,这种服务方式受到了很多业主、公司的欢迎,已有数百家信息服务供应商提供 PM-ASP 服务了。

PM-ASP 服务通常分为如下三种应用的形式。

1) 项目协作平台 (Project Collaboration Network): 这种形式主要用于项目参与各方之间的日常信息交流和协同工作,如文档管理、在线沟通、工作流程的计划控制等。例如主要功能包括:上传、下载、备份文档和设计图纸,版本控制,建立文件访问的日志、在线讨论等。

2) 项目管理门户 (Project Information Portal): 这种形式可提供项目参与各方在项目生命周期种所需的大部分信息,如成本、进度、质量、风险等管理信息。它的主要功能与分布式的项目管理软件类似。

3) 项目采购平台 (Project Procurement Exchange): 这种形式主要用于建设工程项目,可提供建材和服务的电子采购和招投标服务,自动化采购和招投标流程。它的主要功能包括在线浏览产品目录和价格、发出询价单、交换价格数据、网上采购和招投标等。

目前还有一些 PM-ASP 服务供应商将以上的三种模式综合起来,提供了一种完整的服务,称为完整信息门户平台 (Full-Service Portal),这种信息门户平台能够担负起规模较大、时间紧迫、资源有限,项目的各利益相关者在地理位置上距离较远的工程项目。

对于军队的各类工程项目来说,采用完整信息门户平台是一种比较好的选择。这是因为:

- 国防项目的实施每一步都需要采办方、军事代表方的认同和审批,这就需要项目管理门户所提供的各项服务;
- 对于复杂系统的研制,在虚拟领域和半虚拟领域存在很多协同设计、并行设计的问题,需要通过计算机而且系统设计要与使用单位(如列装的部队)、采办单位充分协商才能够最终确定其设计方案,这些工作可通过项目协作平台来完成;
- 而在系统的预研、设计、生产的过程中,

不可能所有的系统组件都要重新进行研制和生产,很多部件都能够采用已有的军用产品,而研制单位可以通过项目采购平台能够查询已有的一些零部件产品或设备,也可以通过采购平台进行网上订货,可提高研制、生产的效率。此外,在一些型号系列比较复杂的领域,如军用电子元器件产品,通过建立已有产品的数据库,在进行新品研制的立项之前进行查新工作,这样就可以避免重复开发某些性能相似的产品。

综上所述,利用完整信息门户平台的关键技术,可以为国防项目提供比较完善的信息服务。然而,军队的信息化项目管理平台在使用方面也应当与商用的信息门户平台有很大不同,这是因为军队的项目管理有其特殊性。

1) 国防采办项目的主要责任者是采办管理机构或合同管理机构,而根据我国的实际情况,这些管理机构将始终负责某一领域内国防采办项目的合同管理,因此采办管理单位将会是信息化项目管理平台的长期使用者,而不是短期的租用。

2) 完整信息门户平台的网络通讯功能对于国防项目至关重要,但是由于安全保密的需要,完整信息门户平台不能够在民用或商业的网络上构建,而必须在军队内部的网络上构建,并需要考虑更多的保密和安全性问题,以免造成泄密。

3) 商业的完整信息门户平台具有一定的时效性,因此它一般不会保留已完成的项目的相关信息。而国防项目的采办具有连续性,有关的国防项目的历史数据对于今后同类项目具有重要的指导意义,因此在国防项目管理信息化服务中,需要提供历史信息的服务。

### 3 国防项目管理信息化服务平台的设计 and 主要功能分析

国防项目管理信息化服务平台主要面向各类国防项目的信息化服务,在这些项目当中承包商可以利用该平台进行项目管理,而项目的采办主管部门则可以通过该平台对项目执行情况进行监控。当项目完成后,与商用的信息化服务平台类似,项目的承包单位就可以停止使用该平台,然而采办主管部门仍然需要利用该平台对其他的项目继续进行管



理,并需要备份储存已完成项目的有关资料,为今后的工作提供借鉴。因此,国防项目管理信息化服务平台的运营主体应当是采办主管部门,而国防项目的承研、承制单位则作为该平台的用户在实施项目时,租用有关的服务。

通过前面介绍的项目管理信息化服务的主要模式以及国防项目的特殊性,可以对国防项目管理信息化服务平台进行设计,其结构示意图如图1所示。

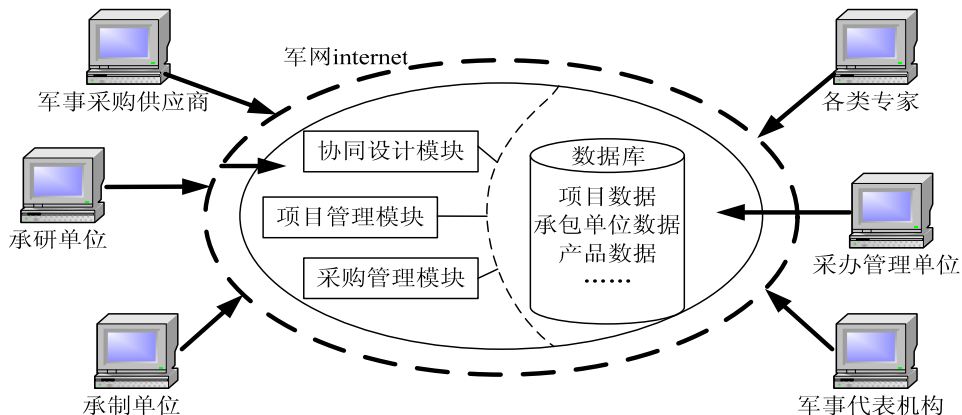


图1 国防项目管理信息化服务平台结构示意图

国防项目管理信息化服务平台主要基于军网internet进行构建,采办管理单位负责运营和维护,承研、承制单位、军事采购的供应商、军事代表机构和军队聘请的各类专家等其他用户都通过军网来接受该平台提供的有关服务,并相互传递信息和文档。

国防项目管理信息化服务平台主要具有四大功能模块。

1) 协同设计模块。对于国防项目这种复杂系统工程而言,必须贯彻并行工程的思想,将复杂产品的功能设计、可靠性设计和保障性设计结合起来成为一个完整的系统工程开发过程。目前国内外先进的系统设计方法,如多学科优化设计方法(MDO)等都提倡计算机辅助的多学科协同设计,因此在国防项目管理信息化服务平台中,采用协同设计模块以实现复杂系统的多学科协同设计功能,为军品的系统工程开发提供技术支持。

2) 项目管理模块。该模块可以实现项目管理软件的所有功能,如进度管理、成本管理风险管理、质量管理、技术状态管理等。除此以外,还应根据我国国防采办的特点,增加立项论证管理、定型管理、产品测试或试验管理等特色服务。

3) 采购管理模块。该模块能够提供电子采购和招投标服务,与项目采购平台的功能类似,可在线浏览产品目录和价格、发出讯价单、交换价格数据、网上采购和进行招投标管理等。

4) 功能数据库。针对前面三个模块的功能,分别建立子数据库。例如,对于协同设计模块,其相应的子数据库应能够调用复杂系统的协同设计信息,进行设计图的版本控制,项目过程中各种设计文档的读取和储存等功能。对于采购管理模块,应提供已有的军品的产品目录、价格信息,并要能够将新研产品的产品信息记入该数据库。除此以外,数据库还应记录各项目的管理过程信息,为以后同类型项目的管理提供历史信息,以便其他的项目承包单位汲取经验教训。

综上所述,国防项目管理信息化服务平台不仅能够实现完整信息门户平台的所有功能,还结合我国国防项目管理的特点,增加一些功能设置。

国防项目管理信息化服务平台与完整信息门户平台类似的功能包括:文档管理、工作流程的自动化、项目通讯录、高级搜索功能、在线讨论、进度管理、成本管理、技术状态管理、权限管理、在线采购和招投标等功能。

而根据我国国防项目的特点,国防项目管理信息化服务平台增加的扩展功能主要包括:

- 系统并行工程设计:专门针对复杂的军用系统,对其功能设计、可靠性设计等进行并行开发,协同设计过程、设计方案的审核等都可以通过网络来进行。
- 定型管理:可进行军品的设计定型、生产定型的管理。传统的产品定型需要召集各

方人员集中开会审查,而信息化服务平台可通过网络进行在线审查,能够提高效率、节约成本。

- 产品查新: 采办管理单位是国防项目管理信息化服务平台的运营主体,他们手中掌握着大量历史产品的资料,如果将这些信息录入数据库,就能够简便快捷地找出用户需要的军用产品。也可以通过该数据库,确定新立项的军品是否与已有的产品重复,以避免不必要的浪费。
- 项目历史数据的收集与整理: 采办管理单位手中掌握了大量已完成项目的信息,这些信息对于未来同类型项目的开发具有重要的参考意义,利用国防项目管理信息化服务平台将这些历史信息收集起来,而且在管理的过程中还能够不断增加历史信息。
- 电子签名服务: 目前我国国防项目在其生命周期全过程中许多审查、考核的手续都是通过文档完成的,这些纸质的文档常常需要通过各级管理部门和领导的签字和盖章才能生效。如果通过网络的信息化服务来传递电子版的文档,必须要用电子签名的形式来替代纸质媒体上的签名和盖章。如果具有这项功能,在项目执行过程中就完全能够实现无纸化办公。

## 4 结论和有待解决的问题

本文针对不断发展的项目管理信息化需求,结合目前我国国防项目管理的实际情况,借鉴了国外现有的工程项目管理信息化服务模式,提出了一种全新的国防项目管理信息化服务平台,并对其主要功能和体系结构进行了分析。这种国防项目管理信息化服务平台能够方便采办管理部门的管理,提高信息传递速度和工作效率,有利于推进项目管理在军队系统的普及和发展。此外,通过信息化服务平台完善的服务,可以实现国防项目全过程的无纸化办公。

但是该平台在具体实现方面还存在一些值得注意的问题。首先,国防项目管理信息化服务平台对于系统和网络的安全性、稳定性提出了更高的要求,很多重大的秘密工程如果采用这种信息化服务平台进行管理,必须要有相应的保密措施。其次,该信息化服务平台是基于军网 internet 的,而军网仅限于军队内部使用,与军队以外的单位之间不能互通,这样不利于外包采办的管理。因此军事采购供应商、承研、承制单位应该和军代表机构进行良好的沟通和协调,由军事代表作为一个中间平台来解决军队与军队以外单位的沟通。此外,对于不同领域的国防采办项目,其项目管理信息化服务可能具有不同的特点,因此在平台系统的开发过程中需要兼顾其通用性和特殊性。这些问题在今后还需要进一步的开展研究。

## 参考文献

- [1] 张勇,李凌楠,谢爽.一种全新的项目管理信息化模式[J].浙江:管理工程学报,2005(增刊):258-262
- [2] 王守清.计算机辅助建筑工程项目管理[M].北京:清华大学出版社,1996
- [3] Ou Xiaohua, Chai Huaqi, Chen Honggen. Integration Management of Enterprises' Effectuating Standards: a Solution Based on ERP Project[C]. Nanjing: Proceedings of the Globalization & Specialization Development of Project Management. 2004
- [4] 沈建明,国防高科技项目管理概论[M].北京:机械工业出版社,2003
- [5] 白思俊主编,现代项目管理(上、中、下册)[M].北京:机械工业出版社,2001

## 作者联系方式

通信地址:合肥市潜山路460号解放军电子工程学院研究生三队

邮政编码:230037

联系电话:13335511300

# 基于ANN的C<sup>4</sup>ISR系统数据融合测试评估

那丹彤 赵维康 张子刚

**摘 要:** 指挥自动化系统(C<sup>4</sup>ISR)作为现代战争中对作战部队和武器系统实施高效指挥与控制的主要手段,其效能的发挥已成为制约部队整体作战效能的关键因素。利用多传感器的资料集成与融合技术把来自多个传感器的资料以及相关情报进行分析和综合处理,对C<sup>4</sup>ISR系统的故障进行诊断定位,提高了系统的有效性和可靠性。人工神经网络为现代复杂大系统数据融合、测试评估及故障定位提供了全新的理论研究方法和技术实现手段。因此,设计了这套基于ANN的C<sup>4</sup>ISR系统的数据融合测试评估系统模型,用神经网络的输出结果与真实情况作比较,得到评价体系定义的性能指标,并根据这些指标综合评估战场态势,定位故障部分,提高系统的有效性和可靠性。

**关键词:** C<sup>4</sup>ISR; 数据融合; 人工神经网络; BP 算法

军队指挥自动化是在军队体系中,综合运用以电子计算机技术为核心的现代科学技术和军事科学,融指挥、控制、通信、情报和电子对抗为一体,实现作战信息采集、传递、处理自动化和决策方法科学化,在现代战争中,是保障对部队实施高效指挥与控制的一种主要手段。C<sup>4</sup>ISR系统是指包含了对抗、计算机、监视、侦察等手段的军队指挥自动化系统。C<sup>4</sup>ISR系统的数据融合测试评估系统是一个极其复杂的非线性系统,客观上要求建立非线性模型。人工神经网络是模拟生物神经元的结构而提出的一种信息处理方法。经过训练的人工神经网络可以把来自多个传感器的资料以及情报进行相关分析和综合处理,得到对战场态势的准确判断,并实时定位故障部分,为迅速恢复C<sup>4</sup>ISR系统功能提供了有效途径。

## 1 评估指标体系

**定义 1:** 在 $T_1—T_2$ 时间内,总共有 $M$ 个目标进入任一传感器的探测范围,其中,进入第 $I$ 个传感器探测范围的有 $N$ 个目标( $N_j < M$ ),经过融合处理判定有 $N_f$ 个目标,其中判断正确的有 $N_r$ 个,则错判为目标的有 $N_f - N_r$ 个:

(1) 目标检出率:  $P_{dc} \lim_{M \rightarrow \infty} = \left(\frac{N_r}{M}\right)$

(2) 目标漏检率:  $P_{dl} \lim_{M \rightarrow \infty} = \left(\frac{M - N_r}{M}\right)$

(3) 目标误检率:  $P_{dv} \lim_{M \rightarrow \infty} = \left(\frac{N_f - N_r}{M}\right)$

**定义 2:** 数据融合精度可以通过融合数据逼近误差来描述,融合数据逼近误差定义为融合后的数据相对于真实数据的误差,可以用各坐标方向的误差及误差均方差来表示。

考虑三维数据,设目标运动的真实数据可描述为 $X(t)=[x(t), y(t), z(t)]^T$ ,其中, $t \in [0, T]$ ,在测试过程中,输入到人工神经网络的数据为 $X(k)=[x(k), y(k), z(k)]^T + V(k)$ ,其中, $V(k)$ 为数据误差,有相应传感器的观测精度和观测噪声给定, $K=1,2,3 \cdots N$ ,采样间隔 $\Delta t = T/N$ ,人工神经网络输出的数据为 $X'(k)=[x'(k), y'(k), z'(k)]^T$ , $K=1,2,3 \cdots N$ ,对应的时间统一基准序列为 $(\tau_1, \tau_2 \cdots \tau_N)$ ,其中, $\tau_N < T$ ,则 $k$ 时刻的数据逼近误差为:

$$e_h(k) = [e_{hx}(k), e_{hy}(k), e_{hz}(k)]^T = [x(\tau_h) - x'(k), y(\tau_k) - y'(k), z(\tau_k) - z'(k)]^T$$

则有:

(1)  $x$  方向的数据逼近误差为:

$$E(e_{hx}) = \frac{1}{N} \sum_{k=1}^N e_{hx}(k), \sigma(e_{hx}) = \sqrt{\frac{1}{N} \sum_{k=1}^N e_{hx}^2(k)}$$

(2)  $y$  方向的数据逼近误差为:

$$E(e_{hy}) = \frac{1}{N} \sum_{k=1}^N e_{hy}(k), \sigma(e_{hy}) = \sqrt{\frac{1}{N} \sum_{k=1}^N e_{hy}^2(k)}$$

(3)  $z$  方向的数据逼近误差为:

$$E(e_{hz}) = \frac{1}{N} \sum_{k=1}^N e_{hz}(k), \sigma(e_{hz}) = \sqrt{\frac{1}{N} \sum_{k=1}^N e_{hz}^2(k)}$$

定义融合数据逼近误差为:

$$E(e_h) = [E^2(e_{hx}) + E^2(e_{hy}) + E^2(e_{hz})]^{1/2}$$

$$\sigma(e_h) = [\sigma^2(e_{hx}) + \sigma^2(e_{hy}) + \sigma^2(e_{hz})]^{1/2}$$

定义 3: 空中目标平均跟踪时间指系统对所有空中目标处于跟踪状态时间的平均值。它是衡量系统的跟踪能力, 即系统掌握空中目标的时间。

$$\text{空中目标平均跟踪时间} = \frac{1}{N} \sum_{j=1}^N \Delta T_j$$

$$\Delta T_j = \frac{1}{N} \sum_{i=1}^{M_j} (Te_{ji} - Tb_{ji})$$

式中:  $N$ ——航迹总数;

$T_j$ ——第  $j$  条航迹跟踪时间;

$M_j$ ——第  $j$  条航迹跟踪段数;

$Te_{ji}, Tb_{ji}$ ——第  $j$  条航迹第  $i$  段跟踪结束,

开始时间。

定义 4: 连续跟踪空中目标系数指系统对所有空中目标处于跟踪状态所占时间比例。它是衡量系统的跟踪效率, 即系统掌握空中目标的连续性指标。

$$\text{连续跟踪空中目标系数} = \frac{T_1}{T_1 + T_2}$$

式中:  $T_1$ ——所有的航迹跟踪总时间;

$T_2$ ——所有的航迹跟踪中断时间。

系统评价的功能组成如下。

1) 情报分系统: 利用雷达、声纳、红外、激光探测设备进行各种情报的探测和获取。

2) 通信分系统: 主要利用卫星通信、微波通信、短波等技术手段进行通信传输完成情报信息和指挥命令的传递。

3) 指控分系统: 用于进行情报综合处理、文电处理、资料检索、图形处理、辅助决策和作战指挥等处理功能。

4) 综合性能系统: 提供对于整个系统供电设备、综合布线等技术支持。保证系统运行的有效和安全。

## 2 人工神经网络

人工神经网络 (Artificial Neural Network, 简称 ANN) 是模拟生物神经元的结构而提出的一种信息处理方法。人工神经网络具有本质的非线性特征、并行处理能力、自适应自学习的能力、联想记忆以及源于神经元激活函数的容错性和鲁棒性 (Robust) 等特点。数学上已经证明, 神经网络可以逼近所有函数, 这意味着神经网络能逼近那些刻画了样本数据规律的函数, 且所考虑的系统表现的函数形式越复杂, 神经网络这种特性的作用就越明显。

人工神经网络, 是从生物学神经系统的信号传递而抽象发展而成的一门学科。在神经网络中, 最基本的单元就是神经元。神经元由三部分组成: 树突、细胞体和轴突。树突是树状的神经纤维接受网络, 它将电信号传递给细胞体, 细胞体对这些输入信号进行整合并进行阈值处理。轴突是单根长纤维, 它把细胞体的输出信号导向其他的神经元。神经元的排列拓扑结构和突触的连接强度确立了神经网络的功能。各神经元之间的连接强度和极性可以有所不同, 并且都可进行调整, 因此人脑才可以有存储信息的功能。图 1 为神经网络的基本结构模型。



图 1 神经网络基本模型

## 3 误差反传训练算法 (BP 算法, Back Propagation)

人工神经网络模型的算法有很多种, 一种典型的算法就是误差反传训练算法, 又称作 BP 算法。本质上, BP 模型是对样本集进行建模; 数学上, 就是一个通过函数逼近拟合曲线/曲面的方法, 将之转化为一个非线性优化问题来求解。

### 3.1 BP 算法的结构模型

BP 算法是一种监控学习技巧, 它通过比较输出单元的真实输出和希望值之间的差别, 调整网络路径的权值, 以使下一次在相同的输入下, 网络的

输出接近于希望值。BP 算法的网络是多层前馈型网络。这种网络不仅有输入层结点，输出层结点，而且有一层或多层隐含结点。对于输入信息，要先向前传播到隐含层的结点上，经过各单元的特性为 Sigmoid 型（收敛型）的激活函数运算后，把隐含结点的输出信息传播到输出结点，最后给出输出结果。BP 神经网络的学习过程分为信息的正向传播过程和误差的反向传播过程两个阶段。外部输入的信号经输入层、隐含层的神经元逐层处理向前传播到输出层给出结果。如果在输出层得不到期望输出，则转入逆向传播过程，将实际值与网络输出之间误差沿原来联结的通路返回，通过修改各层神经元的联系权值，使误差减少，然后再转入正向传播过程，反复迭代，直到误差小于给定的值为止。

### 3.2 BP算法的数学模型

设一个三层 BP 神经网络，网络由  $N$  个输入神经元， $K$  个隐含层神经元， $M$  个输出神经元组成（如图 2 所示）。 $y_{pm}$  和  $O_{pk}$  分别为输出层和隐含层的输出值， $\omega_{2_{km}}$  和  $\omega_{1_{nk}}$  分别为隐含层到输出层和输入层到隐含层的连接权值，设输入学习样本为  $x_{pn}$ ，其对应的希望输出值为  $t_{pm}$ 。

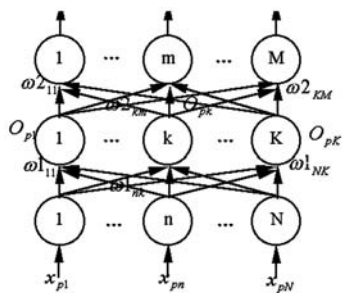


图2 BP神经网络示意图

标准算法步骤如下。

1) 初始化权值，设定学习率  $\mu$ ，允许误差  $\varepsilon$ ，迭代次数  $i$ ，置循环步数  $i = 0$ 。

2) 正向计算：将第  $p$  个样本  $(X_p = \{x_{p1}, \dots, x_{pN}\})$  顺序输入到网络中，按下式分别计算  $O_{pk}$  和  $y_{pm}$ ：

$$O_{pk}(i) = f\left(\sum_{n=1}^N \omega_{1_{nk}}(i)x_{pn}\right) \quad (1)$$

$$y_{pm}(i) = f\left(\sum_{k=1}^K \omega_{2_{km}}(i)O_{pk}(i)\right) \quad (2)$$

激活函数常采用 S 型 Sigmoid 函数： $f(x) = 1/(1 + e^{-x})$ 。

3) 计算均方误差  $E = \frac{1}{M} \sum_{m=1}^M (t_{pm} - y_{pm})^2$ ，若  $E \leq \varepsilon$ ，则停止迭代，否则执行下一步。

4) 反向计算：计算权值的改变量。公式如下：

$$\Delta \omega_{1_{nk}}(i+1) = \mu \sum_{p=1}^P \delta_{pk}(i)y_{pm} \quad (3)$$

$$\Delta \omega_{2_{km}}(i+1) = \mu \sum_{p=1}^P \bar{\delta}_{pm}(i)O_{pk}(i) \quad (4)$$

而

$$\bar{\delta}_{pm}(i) = (t_{pm} - y_{pm}(i))y_{pm}(i)(1 - y_{pm}(i)) \quad (5)$$

$$\delta_{pk}(i) = O_{pk}(i)(1 - O_{pk}(i)) \sum_{m=1}^M \bar{\delta}_{pm}(i)\omega_{2_{km}}(i) \quad (6)$$

更改权值：

$$\omega_{1_{nk}}(i+1) = \omega_{1_{nk}}(i) + \Delta \omega_{1_{nk}}(i+1) \quad (7)$$

$$\omega_{2_{km}}(i+1) = \omega_{2_{km}}(i) + \Delta \omega_{2_{km}}(i+1) \quad (8)$$

(5) 置  $i = i + 1$ ，返回 (2)。

### 3.3 BP算法中的学习率 $\mu$

BP 算法本质上是优化计算中的梯度下降法，利用误差所得到的信息来指导下一步权值的调整方向，以求最终得到的误差最小。为了保证算法的收敛性，学习率  $\mu$  必须小于某一上限。在网络参数中，学习率  $\mu$  是很重要的，它们的取值直接影响到网络的性能，主要是收敛速度。为提高学习速度，应采用大的  $\mu$ 。但  $\mu$  太大却可能导致在稳定点附近振荡，乃至不收敛。针对具体的网络结构模型和学习样本，都存在一个最佳的学习率  $\mu$ ，它们的取值范围一般 0~1 之间，具体取值要视实际情况而定。学习率  $\mu$  影响系统学习过程的稳定性。大的学习率可能使网络权值每一次的修正量过大，甚至会导致权值在修正过程中超出某个误差的极小值而呈不规则跳跃，进而不收敛；但过小的  $\mu$  导致学习时间过长，不过能保证收敛于某个极小值。所以，一般倾向选取较小的学习率以保证学习过程的收敛性（稳定性），学习率  $\mu$  通常在 0.01~0.8 之间。

## 4 数据融合测试评估

由于 C<sup>4</sup>ISR 系统是由指挥、控制、通信、计算

机、情报、监视、侦察等多个系统有机结合在一起形成的复杂系统，其综合效能不仅与每个子系统有关，还与各子系统组成的有机整体密切相关；对这样的复杂系统进行效能评估时，需要进行数据融合测试评估及故障定位。

C<sup>4</sup>ISR 系统数据融合测试、故障诊断定位就是要对 C<sup>4</sup>ISR 系统进行数据融合，在 C<sup>4</sup>ISR 系统出现故障时及时的对故障点进行定位，查找故障原因。而基于 ANN 的 C<sup>4</sup>ISR 系统的数据融合测试评估系统经过训练和学习之后，可以根据传感器传递到系统模型的信息更加准确地判断出各故障的具体位置或各部分器件出现故障的可能性。在对 C<sup>4</sup>ISR 系统实际工作和维修情况做了初步的了解和调研论证之后，本文考虑以下几种故障现象作为该系统的初始化样本：情报分系统故障、通信分系统故障、指控分系统故障、反应综合性能系统故障。具体情况如表 1 所示（其中 X<sub>i</sub> 表示故障代码）。

表 1

X <sub>1</sub>	情报分系统故障	X <sub>2</sub>	通信分系统故障
X <sub>3</sub>	指控分系统故障	X <sub>4</sub>	反应综合性能系统故障

同时考虑造成以上故障现象的故障原因：情报的时延、情报的容量、通信误码率、通信吞吐量、通信的时延、综合处理信息时间、信息总体质量、决策所需时间、系统的抗毁性、系统的隐蔽性、系统的互通性以及一种特殊情况（系统正常）。具体情况如表 2 所示。（其中 Y<sub>i</sub> 表示特定故障的代码）

表 2

Y <sub>1</sub>	情报的时延	Y <sub>2</sub>	情报的容量
Y <sub>3</sub>	通信误码率	Y <sub>4</sub>	通信吞吐量
Y <sub>5</sub>	通信的时延	Y <sub>6</sub>	综合处理信息时间
Y <sub>7</sub>	信息总体质量	Y <sub>8</sub>	决策所需时间

表 3 输入输出结果

网络输入				网络输出											
X <sub>1</sub>	X <sub>2</sub>	X <sub>3</sub>	X <sub>4</sub>	Y <sub>1</sub>	Y <sub>2</sub>	Y <sub>3</sub>	Y <sub>4</sub>	Y <sub>5</sub>	Y <sub>6</sub>	Y <sub>7</sub>	Y <sub>8</sub>	Y <sub>9</sub>	Y <sub>10</sub>	Y <sub>11</sub>	Y <sub>12</sub>
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0.93	0.19	0	0	0.41	0.37	0.08	0.09	0.05	0	0	0	0	0	0	0
0	0.96	0	0	0	0	0.67	0.13	0.2	0	0	0	0	0	0	0
0	0.12	0.95	0	0	0	0.09	0.03	0.05	0.17	0.55	0.11	0	0	0	0
0	0	0	0.89	0	0	0	0	0	0	0	0	0.37	0.22	0.41	0

续表

Y <sub>9</sub>	系统的抗毁性	Y <sub>10</sub>	系统的隐蔽性
Y <sub>11</sub>	系统的互通性	Y <sub>12</sub>	系统正常

建立一个三层的 BP 网络，在网络之中，把 4 种分系统故障作为神经网络输入层的节点，11 种故障原因作为输出层的节点，同时把隐含层的节点选为 10 个，通过对传感器传递到系统的大量的原始数据进行数据融合后，对人工神经网络进行训练（即适时的修改网络的各个连接权值）后，可以使输入值与输出值之间获得一种相对的稳定，即使造成每一种故障的原因明确化，达到诊断故障的目的。

BP 神经网络模型计算所使用的软件和程序是 MATLAB 神经网络工具箱。神经网络工具箱的使用，可以大大方便权值训练，减少训练程序工作量，有效的提高工作效率。建立 MATLAB 神经网络模型进行故障诊断系统的试验：net = newff（minmax（pn），[10，12]，{'tansig'，'purelin'}，'trainlm'）；其中 newff()是建立的 BP 神经网络的函数，minmax（pn）表示样本数据经预处理后的网络输入 pn 的取值范围，[10，12]表示隐含层节点数是 10，输出层节点数是 12，{'tansig'，'purelin'}表示隐含层中的神经元采用 tansig 转换函数，输出层采用 purelin 函数，'trainlm'表示选择的学习算法。然后进行权值和阈值初始化 net=init（net）；给各连接权值 IW{1，1}、LW{2，1}及阈值 b{1}、b{2}赋予（-1，+1）间的随机值。学习过程[net，tr]=train（net，pn，tn）；根据网络学习误差逆传递算法得到新的网络权值及阈值。最后是模拟 an=sim（net，pn）；a = poststd（an，meant，stdt）；根据训练好的网络及输入向量进行模拟网络输出，结果如表 3 所示。

在输入端的输入节点表示传感器传递过来的数据经融合后作为分系统出现的故障现象的原始样本初值,并把各种故障进行归一化处理,使  $X_i$  的数值始终处在[0,1]之间来表示故障的严重程度,其中 0 表示没有  $X_i$  所代表的这种故障,1 表示这种故障已经无法修复。而输出端的输出节点则表示特定的故障原因,其输出值代表该故障发生在该部分的可能性量度,当同时出现多种故障时,输出值越大表示该部分发生故障的可能性就越大;相反,输出值越小时该部分发生故障的可能性就越小。例如,当所有的输入值都为零时,说明  $C^4ISR$  系统此时没有故障,系统一切正常,所以网络输出均为 0;当通信分系统出现故障时,通信中的误码率是最有可能造成此种故障的原因。

## 5 结语

经过对  $C^4ISR$  系统的数据融合测试评估及故障诊断的 BP 神经网络试验后,得出的训练结果与实测值相差较小,表明用 BP 神经网络方法对  $C^4ISR$  系统进行数据融合测试评估、故障诊断定位的可行性。数据融合过程实现了分布式融合计算,融合测试过程根据人工神经网络的误差反转算法,依次调用各个传感器数据,最后将测试的相关信息及融合过程中所产生的各种输出结果进行分析、比较、评估,诊断故障点,保证  $C^4ISR$  系统有效可靠地运行。

## 参考文献

- [1] 杨立生. 军队自动化指挥系统.北京:国防工业出版社,1994.10
- [2] Simon Haykin; 叶世伟,史忠植译.NEURAL NETWORKS.神经网络原理.北京:机械工业出版社,2004.1
- [3] 焦李成. 神经网络系统理论. 西安:西安电子科技大学出版社,1995.3
- [4] 韩利竹,王华.MATLAB 电子仿真与应用. 北京:国防工业出版社,2003.9

## 作者联系方式

通信地址:长春市花园路1号解放军装甲兵技术学院电子工程系通信教研室

邮政编码:130117

联系电话:13009138570 0431-86983416

# 无线射频技术实现战场维修资源信息一体化

沈云秋 赵韶平 殷维刚 张立新 常波

**摘 要:** 研究战场集装箱物资的可视化识别和管理技术。运用无线射频技术,可自动识别各集装箱物资信息,并通过无线射频通信可实时更新集装箱物资清单信息。建立战场物资可视化系统。

该系统更新数据将实时同步至远程数据库服务器。

**关键词:** 无线射频; 战场维修; 资源可视化

## 1 引言

在经济全球化和信息化的推动下,现代军事物流已经从为军队提供传统的运输服务,发展成为以现代科技、管理和信息技术为支撑的综合军事物流服务。以物流部门为主体、由运输和信息两大平台构成,涉及生产、流通和仓储过程的现代军事物流系统,已发展成为适应当今军事领域最新发展趋势的重要基础环节。其中,集装箱运输和堆放管理作为现代军事物流的一个重要组成部分,在现代战争后勤保障、运输体系中发挥着重要的作用。随着美军两次伊拉克战争的结束,“全球军用物资可视化”的概念,以及其在战争发挥的作用,备受世人的关注。

我国作为世界军事领域的强国,面对当今军事领域最新发展趋势,集装箱物资、堆场和通道如何建设物流多媒体信息高速走廊,推广信息化技术,建立数字信息平台,提高物流信息的搜集、处理和服务能力,缩短物流信息交换与作业时间,已经成为急需解决的问题。为适应现代化战场对武器装备技术保障精确化、透明化要求,本项目利用无线射频技术实现战场维修资源信息一体化,开发战场物资自动识别登记卡,用于快速、查寻、识别和监控集装箱内物资信息,极大地提高物资保障的速度和准确性,具有重大的经济和军事效益。

## 2 战场维修资源信息一体化总体概述

战场维修资源信息一体化是可视化系统的重要

组成部分。该系统主要针对战场上集散物资(集装箱物资和堆放物资)实施快速可视化识别、监控和管理。战场上维修物资一般进行集装箱化包装,对于集装箱物资自动识别将采用无线射频识别技术。本系统运用两级无线射频通信,使用户能实时跟踪目标集装箱的位置,能实时识别、监控、查寻集装箱内物资的品名、数量和位置等相关信息。

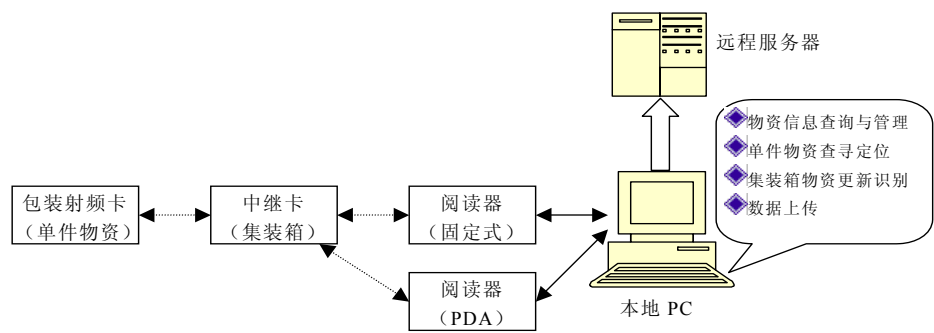
## 3 战场维修资源信息一体化组成结构

为满足物资识别、监控和管理目标,系统构建了软硬件集成方案。系统硬件由包装射频卡(有源单向 tag)、双向射频卡(双向 tag)、集装箱货单射频卡、手持式或固定式阅读器、上位机组成。系统软件分上位机(PC 机)软件和 PDA 软件(PDA 软件可在 PC 机软件模块基础上部分裁剪)。系统总体架构图及硬件结构图、软件结构图分别见图 1、图 2、图 3。

## 4 工作原理及流程

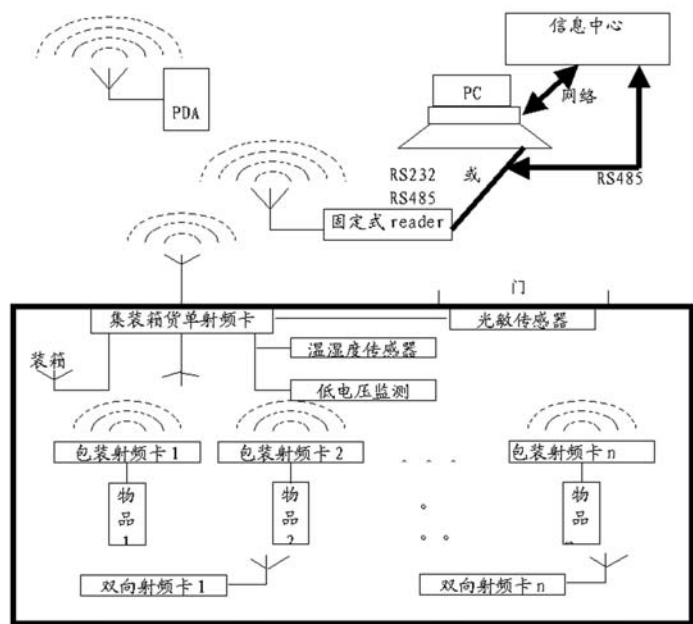
包装射频卡为单向的 tag, id 号为 4 个字节。出厂时所有 tag 的 id 号均为 FF FF FF FF,可以通过写卡器更改 tag 的 id 号码。使用过程中,通过写卡器修改 tag 的 id 号,并把 tag 的 id 号和物品的名称之间的对应关系登记在后台数据库内,其原理框图见图 4。





- 注：1. 中继卡具有应答包装射频卡、数据存贮和射频发射功能。以下称“数据库货单射频卡”。  
2. 图中虚线表无线通信，实线表有线通信。  
3. 本地 PC 数据通过广域网上传至中心服务器。

图 1 系统总体架构图



注：光敏传感器控制集装箱货单射频卡的工作启停，出于节能考虑。

图 2 系统硬件结构图

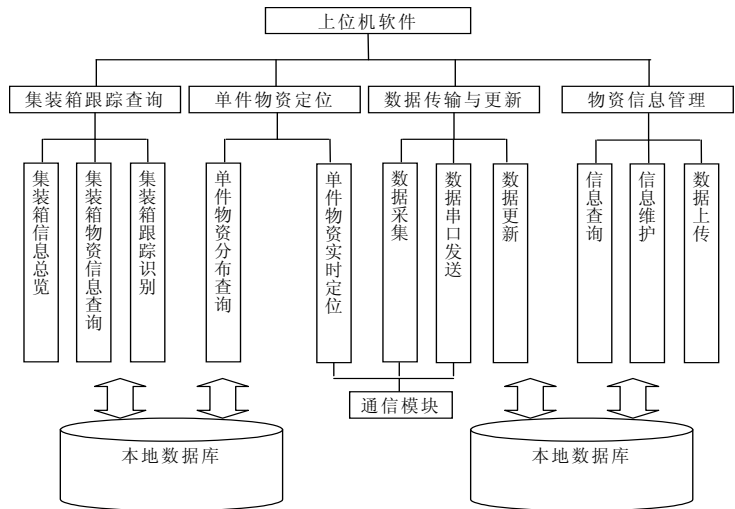


图 3 系统软件结构图

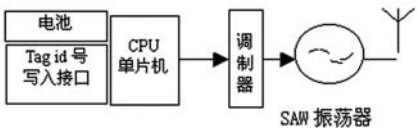


图 4 包装射频卡原理框图

Tag（即包装射频卡）一旦安装在物品上，就成为物品的固有属性，相当于该物品有了一个固定的 id 编号。在后台数据库内，每件物品都有自己唯一的包装射频卡 id 号。为了方便管理，物品上安装一个包装射频卡后，包装射频卡不可以轻易脱离物品，不可以随意把包装射频卡拆卸，再安装其他种类的包装射频卡。若想将物品上的射频卡换成别的射频卡（id 号不一样），必须把物品的名称等属性和射频卡的 id 号在后台数据库内重新登记。

使用过程中，集装箱阅读器部分把集装箱内的物品的 id 号读取之后，保存在和数据库货单射频卡共用的存储区内，数据库货单射频卡部分根据上位机的指令（手持式 reader 或固定式 reader）把自

身的 id 号和集装箱内物品的 id 号传给手持式 PDA 时，手持式 PDA 利用内部数据库的对应关系，把集装箱内物品的 id 号翻译成物品名称，通过 PDA 上的 LCD 显示器显示出来，同时也可以统计出物品的个数，物品的种类个数，以及物品的总个数。如果 PDA 内存有该集装箱内以前的物品信息即历史数据，可以把历史数据和当前数据进行比较统计出之间的差别，相当于告诉用户该集装箱内多了什么物品或少了什么物品。

同样的道理，数据库货单射频卡把自身的 id 号和集装箱内物品的 id 号通过固定式 reader 上传给 PC 机后，利用 PC 机上的应用软件，也可以对集装箱内的物品进行统计。其原理框图见图 5。

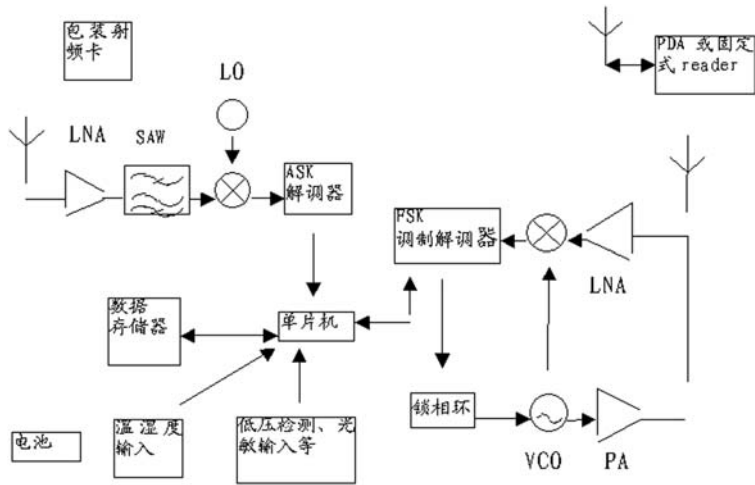


图 5 集装箱货单射频卡原理框图

双向的射频卡定时唤醒接收集装箱货单射频卡中的数据库货单射频卡部分发送的指令，根据指令，发送包装袋的物资信息（物资名称，种类等信息），或者接收手持式 reader 的查询指令（主要根据物资名称，编号等），若收到和自身保存的物资信息一致的指令时，就启动蜂鸣器报警，提醒用户物资的存在位置。

5 关键技术及解决措施

- (1) 远距离数据采集技术  
系统采用有源电子标签及提高发射机功率的方法，使识别距离达 100m 以上。
- (2) 两级无线射频通信技术  
系统采用两级无线射频通信，成功实现了货单射频卡与包装射频卡、包装射频卡和应答机之间的

射频通信。

(3) 发射机、接收机技术  
发射机的目的是调制基带数据，然后上变频到射频，同时需要充分的功率放大，不能产生信号失真和邻近信道干扰。接收机的功能是在强干扰和噪声存在的情况下能成功解调所需要的信号。系统采用零中频接收机方案，和超再生接收机相比，零中频检测接收机具有实现简单，成本低的优点，并且其接收灵敏度也可以满足系统要求。

(4) 防碰撞技术  
射频识别中防碰撞技术也称多目标识别技术。当在货单射频卡的天线区域中及集装箱内有多个包装卡同时到达时，它们几乎同时响应读写器的指令而发送信号，这样就会产生信道争用的问题，信号互相干扰，包装射频卡不能正确接收数据，也就不能正确识别包装卡。应答机与货单射频卡亦产生同样的信号碰撞问题。在系统的非接触识别过程中，

利用防碰撞技术同时完成目标识别，满足了一些特殊场合的需要，扩大了识别技术的应用范围，提高了工作效率。

#### （5）信息安全及加密纠错技术

系统的安全性是系统设计中需要考虑的问题。尤其因为系统采用射频方式工作，对数据的保护更为重要。在系统设计中用多种办法对数据保护。包装射频卡的序列号的唯一性，包装射频卡和货单射频卡及应答机间的相互认证，使用数字签名方法以分清责任，还使用纠错和加密相结合的办法来传输数据，既保护了数据又降低了系统的复杂性。

## 6 结束语

无线射频识别在未来装备管理中具有巨大的发展潜力。目前，美国国防部已经在内部使用该系统，跟踪大约 40 万件物品，从集装箱到蜂鸣器都有。作为一种进行集装箱远程跟踪的解决方案，射频识别还将进一步广泛应用于国防领域的物流系统中，极大地提高物资保障的速度和准确性，具有重大的经济和军事效益。

### 参考文献

- [1] 无线射频识别（RFID）与条码技术. 北京：机械工业出版社. 游战清，2007.1
- [2] 射频电路设计. 北京：电子工业出版社. Joseph J.Carr. 2001.10
- [3] 现代物流装备与技术实务. 北京：人民邮电出版社. 李文斐，张娟，朱文利，2006.10

### 作者联系方式

通信地址：北京市清河大楼子 8 二炮装备研究院三所

邮政编码：100085

联系电话：010-66345298

# 多机空战决策融合实现技术研究是实现

史进 严丽娜 秦国强

**摘要:** 本文研究了空战中的决策融合问题。对空战决策融合的态势评估和威胁估计进行了深入分析,建立了决策融合的实体多 Agent 模型,为多机协同空战指挥自动化发展提供了新思路。

**关键词:** 决策融合; 态势评估; 威胁估计

为了复杂环境下充分利用各战机传感器资源,最大限度挖掘武器性能,需要在不同信息层次上融合不同有效信息。即数据融合包括检测融合,状态融合,属性融合和决策融合四个层次。决策融合是最高层次的信息融合,它以符号推理为主,实现人的推理、判断、决策功能,达到指挥控制自动化,提高武器系统的作战效能、反应速度和生存能力。

## 1 空战决策融合分析

从决策学的角度看,多机空战的决策空间是由若干个拥有某个领域或者区域不同决策权力的决策单元组成的<sup>[1]</sup>,决策单元就是战场中的战斗机或者战场外的预警机等,其本质是一种分布式多 Agent 决策过程。其特点如下。

### 1.1 决策问题复杂性

多机空战面临的是由诸多相互关联、相互制约的因素构成的复杂而且缺少足够数据的决策空间,是复杂的不良结构化问题。由于各决策者占有信息的局部性以及决策能力,决策权力的局限性,它们对整个空战态势缺乏整体,宏观的认识,难以避免决策中大量存在的冲突,整个决策问题十分复杂。

### 1.2 决策信息分布性

由于多机空战中各决策者(飞行员)自身获取信息的能力是有限的,每个决策者掌握的信息只是整个空战态势的局部,因此,整个态势使若干个局部信息的集合,在地理上分布于各个决策者的局部空间中,这种信息的分布性有可能使决策者因为信

息不足而决策失误。为了避免这种失误,各决策者之间需要通过信息共享来扩充自身的决策信息。

### 1.3 决策过程层次性

在一个不考虑空中预警机或者地面指挥的情况下,多机空战的决策问题涉及到三个层次:第一层次是编队内各飞机对自身占有局部情况进行局部信息融合,并向本方长机报告;第二层次是带队长机在综合各僚机的局部情况的基础上,得到空战的整体态势,给编队中各僚机分配攻击目标;第三层次是编队中某战斗机在接受分配的目标后,进行相应的单机战术动作。整个多机空战决策过程就是这三个层次决策的有机结合。

## 2 决策融合分类

决策融合包含态势评估(Situation Assessment, SA)和威胁评估(Threat Assessment, TA)。

### 2.1 态势评估

态势评估是对战场上战斗力量分配情况的评价过程<sup>[2]</sup>。它根据对各种作战平台身份识别的结果,通过综合敌我双方及地理、气象环境等因素,将所观测到的战斗力量分布与活动和战场周围环境、敌人的作战意图及敌机动性能等有机结合起来,分析并确定事件发生的深层原因,得到关于地方兵力结构、使用特点的估计,及时、准确地给出一个战场态势的动态描述,最终形成战场、空情的多维态势图。态势评估包括态势提取、态势评价、态势预测,如图 1。

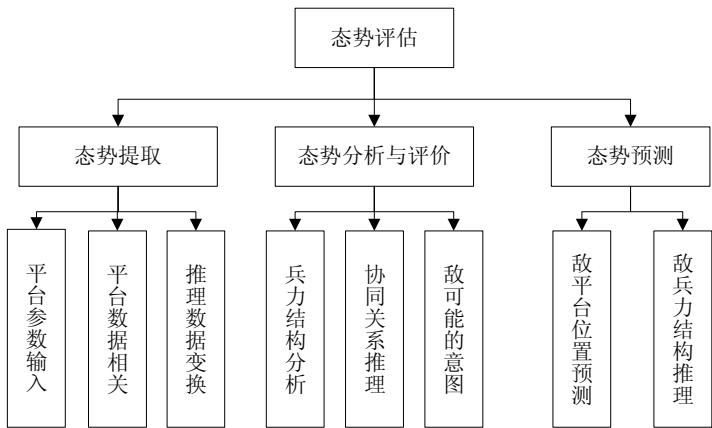


图 1 态势评估结构框图

态势提取主要完成当前敌我平台、各实体参数（如类型、数量、位置、速度）的提取、相关、识别及推理数据的变换。态势评价主要完成兵力结构分析、协同关系推理及行为意图推理。态势预测主要完成敌实体（或平台）未来位置计算和敌方兵力未来部署的推理。

2.2 威胁评估

威胁评估是以态势评估的全部结果为背景，综

合地方的破坏能力，机动能力和行为意图，做出关于敌方杀伤能力和对我方威胁程度的评估。威胁评估根据敌我武器性能、敌方电子设备性能、我方重点保卫目标、我方电子设备性能、敌我双方作战策略的知识，尽可能以定量的形式对敌方兵力威胁程度做出分析，并提出应采取战术对策的辅助决策供指挥中心参考。威胁评估包括综合环境判断、威胁等级判断、战术辅助决策，如图 2。

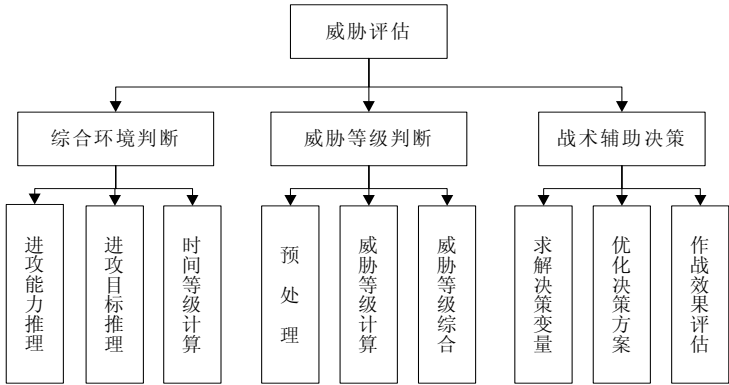


图 2 威胁评估结构框图

综合环境判断主要完成进攻能力的推理、进攻目标推理、进攻时间推理。威胁等级判断主要完成威胁等级计算及威胁等级综合<sup>[3]</sup>。战术辅助决策主要用于指导机载武器系统作战计划生成，给驾驶员推荐进攻或防御计划，使驾驶员能够在最佳时机和最佳位置对目标实施攻击或使驾驶员能及时改变飞行航线计划以规避敌方的攻击。战术辅助决策最终要用快速交战模型进行评估，该模型能够估计出假想的战斗结果。

3 基于多Agent模型的实现技术

针对多机协同空战的决策融合问题，需要建立决策融合的实体 Agent。战场中的每一架飞机都是多 Agent 系统中的一个计算实体。同时需要建立个体智能 Agent 的结构模型以及智能 Agent 的环境感知模型、期望模型、意图模型和协同中的通讯行为。其系统的总体结构如图 3。

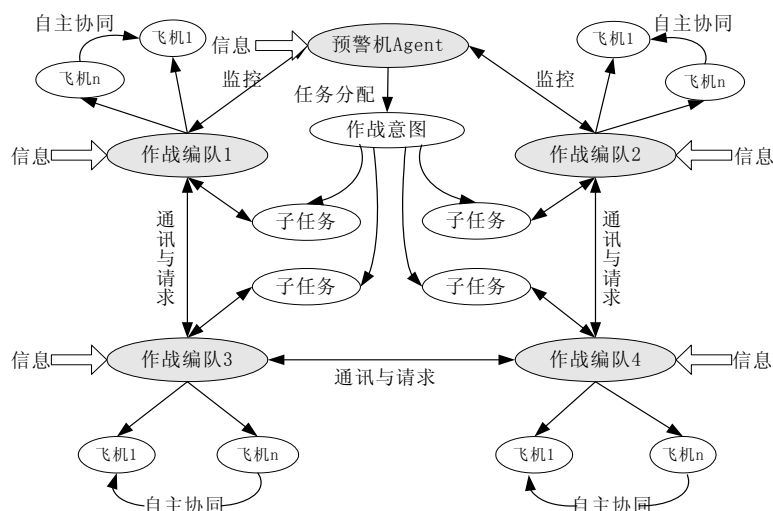


图3 多机协同空战总体结构

整个系统由预警机和多个作战编队组成。预警机负责对战区敌方信息进行探测, 监控我方战机, 制定出作战意图, 分配作战任务并进行编队间的协同。各编队根据初始任务和指令协同方案与友机和预警机保持联系, 不断探测战场态势, 实施新的自主协同攻击。在各编队中, 一架飞机担任长机, 其余的飞机执行协同任务。

对个体智能 Agent 战机而言,其系统结构有 4 大模块组成,这就是环境感知模块,期望模块、意图模块和执行机构,如图 4。

环境感知模块即 Agent 的信念部分，提供 Agent 决策的信息，由态势评估、时间探测、态势预测组成。

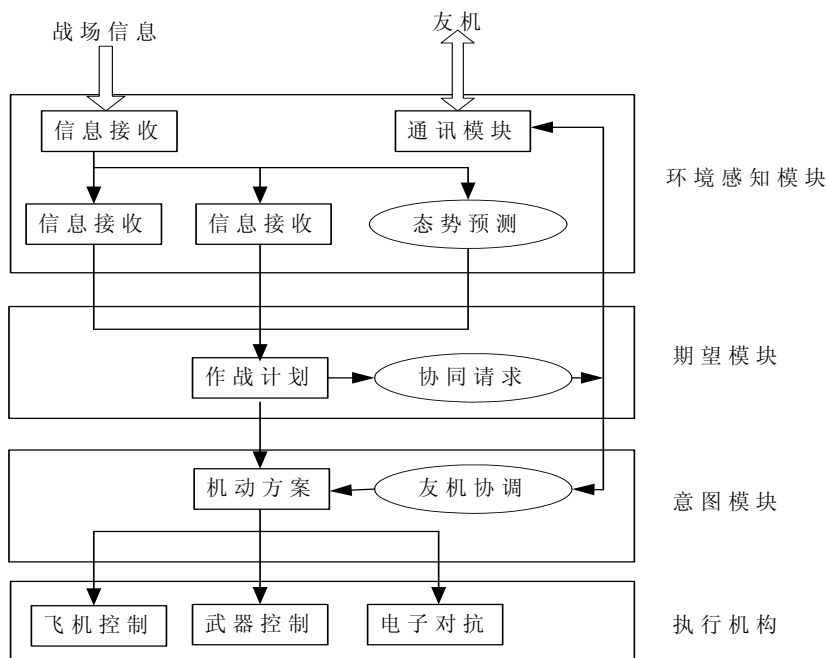


图 4 个体 Agent 模块结构

期望模块即 Agent 的期望部分，表示 Agent 的动机。根据敌机当前的态势、机动意图及下一步可能的决策等信息制定出作战计划，如目标分配、自主协同攻击方案、向友机的协同请求等。期望目标

的类型如下。

实现攻击任务：初始攻击和再次攻击的目标选择与分配，请求友机支援和配合友机实施策应、实施协同的联络方式等。

实现防御任务：包括电子干扰的实时投放及大机动过载规避。

退出攻击：根据我机状态及威胁状态，及时退出攻击或跳伞救生。

意图模块根据自主协同攻击方案及友机协同决策信息，选择相应的攻击或规避决策，并将决策信息输出到相应的控制机构，如飞行控制机构，武器控制系统，电子战系统等。意图模型的具体决策有：

攻击目标和路径的选择、攻击武器的选择发射时机控制等。

协同战术的选择、协同中任务分配等。

电子干扰的投放及规避动作的选择。

退出攻击的路线选择和跳伞时机的选择。

执行机构是实现协同攻击的关键，而 Agent 之

间的通讯尤为重要。通讯的实现主要包通讯信息与通讯行为；通讯信息主要是指协同攻击中最小信息共享集；通讯行为有请求、承诺、通知等。

## 4 小结

本文研究了一种基于多 agent 模型的实现技术，但由于空战中的决策数据量大，决策因素的不完整、不确定、不一致甚至矛盾造成了决策融合的复杂性。因此，决策融合技术需要综合运用多种方法论、建立大量的专业支持数据库才能够进一步完成整个决策过程，从而为空战决策自动化提供更有力的技术支持。

## 参考文献

- [1] 吴杰, 信息融合技术在战略决策支持系统中的应用[J], 科技广场, 2007, 23 (1)
- [2] 荔建琦. 进化决策的模型、关键技术与应用研究[D].长沙: 国防科技大学.2002
- [3] 董彦非, 冯惊雷, 张恒喜.多机空战仿真协同战术决策方法.系统仿真学报[J].2002, (5): 723-725.

## 作者联系方式

通信地址：西安通信学院一系通信与指挥自动化教研室

邮政编码：710068

联系电话：029-84706479      13891961365

# 军校教学保障信息化建设理论与实践研究

孙厚钊 任训平

**摘 要：**从军校教学保障信息化建设的特点、教学保障信息化建设的原则、教学保障信息化建设的方法等方面论述了军校教学保障信息化建设的理论基础，最后给出了一个军校教学保障信息化系统实例。

**关键词：**教学保障；信息化；信息化建设理论

随着信息技术在军校教学、科研、管理等多领域的广泛应用和发展，军校教学保障工作也踏上了信息化发展的“快车道”。研究和把握教学保障信息化的特点、原则和要求，探索教学保障信息化的机制、方法和手段，对于揭示军校教学保障信息化建设活动的规律，认真做好教学保障工作，发挥军校教学保障信息化建设的最大效益，具有重大的现实作用和意义。

## 1 军校教学保障信息化建设的特点

在信息化条件下，军校教学保障信息化建设已在一定程度上从后台走向了前台，在功能和属性上呈现出主动性和技术性的特征，表现了新的特点。

### 1.1 保障的范围和内容扩大

从教学保障工作看，为了培养大批适应未来信息化战争的信息化人才，军校教育信息化首先是教学信息化。教学信息化必然将在教材、装备和物资器材、教学设施和教学勤务等方面给保障工作带来许多新的任务和要求，使得教学保障的范围更加广泛，内容大大拓展，情况更趋复杂。

### 1.2 保障的手段更加先进

#### 1.2.1 保障的技术含量不断增大

未来信息化条件下的军校将是一个“信息化校园”，军校教学、科研和生活保障将朝着信息系统化和系统信息化的方向发展，信息化的保障将不仅仅限于信息的传播，而是深入到教学、科研和生活的深层领域，在深刻改变教学、科研和生活的同时，也深刻改变着保障工作自身。随着保障的技术

含量在军校信息化的进程中不断增大，技术要求不断增加，军校保障的技术要求将突破简单的“收发发”、“修修补补”，而是向着满足系统化地建设信息化校园和培养信息化军事人才需求的方向发展。

#### 1.2.2 保障的时空得到扩展

军校教学保障信息化建设在保障范围和内容大大扩展的同时，保障的时间和空间跨度也得到了扩展。在时间上，由于计算机强大的数据处理功能，保障人员可以对已经完成过的各项保障工作做到有序整理和存档，并对过去的保障工作进行科学分析，及时总结经验教训，并在需要的时候从已有的保障工作中及时提取有用的信息，并利用计算机的分析计算能力，科学地预测未来保障工作的需要，做到科学预测、有的放矢，为保障工作计划提供指导。在空间上，信息化条件下的军校校园是一个多种信息的整合体，信息化条件下的保障工作将涉及到军校内部的各个机关、教研室等职能单位。

### 1.3 保障的方式趋于多样

军校保障信息化正在日益突破传统的单一保障模式，向着集约化的复合保障模式发展。随着军队装备和后勤体系的调整，要求优化保障要素，建立高度联合、综合集成的保障体系，在军校逐步实行社会化保障。军校作为军事系统整体的一部分，作为培养适应信息化战争需要的军事人才的基地，必须适应时代发展要求，不断进行改革创新，充分依托国家综合国力，综合运用军队和地方的各种资源，对教学和生活提供最优化的保障。现阶段军校的保障方式将进一步推进传统的保障形式与现代保障形式的结合，军队体系保障与地方社会化保障的



结合,实现保障方式多样化。

## 1.4 保障信息丰富及时

随着信息爆炸这一时代特征的出现,新的知识信息无时无刻不在大量地产生,其发展变化之快令人目不暇接。军校教育在走向信息化的过程中给教育各方面都带来了信息巨变,军校教学保障信息化建设也不例外。

## 1.5 对保障人员的信息素质要求提高

由于网络和计算机技术大量运用于保障工作,军校教学保障正由人力密集型逐步向科技密集型转变,各种信息化教学设备及训练器材的大量使用,使得原来主要依靠体能、技能来完成军校保障任务的人员,逐步被众多主要依靠智能来完成军校保障任务的专业人员所代替。因此,军校教学保障信息化建设工作要求完成各类保障任务的全体人员,必须了解一定的市场经济知识、现代管理知识、现代科技知识,特别是要具备良好的信息素养,具备娴熟的业务技能,以适应信息化条件下保障工作的需要。

# 2 军校教学保障信息化建设的原则

军校教学保障信息化建设要以军校教学改革的总体目标为依据,紧密结合各项保障工作的实际,以信息技术为核心的现代科技为根本推动力,不断探索军校教学保障信息化建设的基本规律,改革创新保障方式,优化保障手段,强化保障能力,注重保障效益,实现优质服务,在实践中走出一条军校教学保障信息化建设的新路。

## 2.1 实行“一体化”保障

所谓“一体化”保障,是指在信息化条件下,对军校的全部保障工作实施跨单位、跨部门的集中统一规划、统一调度,科学预测保障需求,以减少损耗,提高保障效益。军校教学保障信息化建设要着眼实现保障结构的合理优化,搞好政策制度的配套改革,以教育信息化条件为基本纽带,积极推进军校相关保障部门的保障一体化建设,从而真正实现军校教学保障信息化建设的高效益。要推进保障

工作的一体化,首先要加快保障信息的一体化建设,如构建一体化的信息支撑平台,建立友好的协作机制,实现公共保障信息的互联互通和共建共享等。

## 2.2 实行“精确化”保障

在信息化条件下,信息已成为提高军校保障力的关键因素。由于不断发展的新技术提供了对保障对象透彻的技术分析,使得保障单位和人员能够对保障对象、保障时间、保障地点、保障内容等要素有准确的把握,从而使保障工作方式由传统的“粗放型”逐步向信息化条件下的“精确化”过渡。

## 2.3 实行“快速化”保障

所谓“快速化”保障,是指利用横向扁平的网络化信息系统打破传统的纵向条块分割的信息传播模式,使信息在保障部门及其人员之间与被保障部门及人员之间实现快速流动。同时,由于信息技术提供了先进的信息处理和传播手段,使得保障工作具备了及时分析保障需求、快速保障需要的能力,提高了保障工作的时间利用率,尤其是能够充分应对动态的保障需求。信息化的保障手段克服了传统手段的被动性,实现了保障的主动应对,从而实现保障工作的快捷便利和及时高效。

## 2.4 实行“透明化”保障

“透明化”保障是指利用信息网络的公开性达到保障信息的高度共享,通过保障实施者与接受者的及时互动,实现教职员工对于军校教学保障信息化建设的群众性参与,以保证保障工作的公开、公正。传统的保障工作由于办公手段的落后和部门间的阻隔,信息通常被封闭在一定的范围内,各部门、各单位往往难以了解保障工作的全面情况,也很难对保障工作及时提出合理化的建议。因为缺少群众的理解和支持,使得传统的保障工作经常出现脱离需求、“出力不讨好的”情况。而信息时代保障工作将置身于一个开放的社会环境,保障工作能综合社会的力量,得到社会化的保障力量的支持。军校教学保障信息化建设彻底地改变了过去单打独斗的被动局面,使“透明化”成为其最基本的特征之一。

## 2.5 实行“规范化”保障

所谓“规范化”保障,是指针对军校教学保障信息化中不断出现的新特点和新要求,军校必须加强对信息化保障工作特点和规律的研究,不断规范军校教学保障信息化建设的运作机制,使新的条件下的军校教学保障信息化建设有章可循、有法可依。事实上,在教育信息化的进程中,信息化在使军校教学保障信息化建设的方式和手段不断拓展的同时,也给军校教学保障信息化建设带来了许多新的问题和挑战。例如军校教学保障信息化建设具有开放性、灵活性的优点,但同时也使重要信息的保密工作面临新的考验。军校教学保障信息化建设的开放性、灵活性,并不意味着随意性和盲目性,所以军校教学保障信息化建设必须以特有的方式和制度调控自身的运行,使之成为有目标、有管理、有评价、有反馈、有调控的规范活动。

## 3 军校教学保障信息化建设的方法

随着军校教学保障信息化建设要求的不断提高以及保障难度的不断加大,必须加大保障工作改革力度,创新保障工作模式,针对新的特点和要求,着眼于提高信息化保障工作效能,以创新的方法手段不断开拓军校教学保障信息化建设的新局面。

### 3.1 加强信息化保障工作的组织协调

为了快速高效地满足信息化教学、科研、管理、后勤等工作需求,军校信息化保障工作迫切需要加强组织领导和协调,在各级首长和相关部门的领导下,加强保障工作职能部门的建设,努力建设一支熟悉信息化保障工作任务和特点的专业性管理队伍,并不断提高一线保障人员的信息化保障素养,强化信息化保障能力,优化工作流程,确保保障工作效能。

### 3.2 搭建信息化保障的系统平台

做好军校教学保障信息化建设,必须提高保障工作自身的信息化水平。在加强军校网络基础设施建设的同时,要下大力气搭建信息化保障的系统平台,使军校信息化保障置身于一个网络化、智能化、数字化的保障环境中。

## 3.3 建立信息化保障评价机制

建立军校信息化保障水平的测量与评价的科学方法,设置军校信息化保障水平评价的参考指标体系,客观评价军校信息化保障水平,比较军校在信息化保障发展水平方面的差异和特点,对于军校制定正确的信息化发展策略,有针对性地改进和提高信息化保障水平具有重要的意义。

## 3.4 确保信息化保障的安全

信息安全问题是军校教育信息化的突出问题,保障工作的信息安全也成为军校保障信息化面临的首要难题之一。信息安全通常包括机密性、完整性、可用性和可控性四个方面。当前,信息化保障面临的信息安全问题不仅是军校教学保障信息化建设的内部问题,更关系着军校教学、科研、管理等各项工作的安全运行和正常开展。军校必须将保障信息的安全运行置入军校安全工作的整体工作中。平时,在加强严格管理和做好技术防范的同时,应制定信息化保障应急处置方案。该方案应切合本单位的实际情况和当前的技术发展趋势。具体地说,处置方案应包括实体安全(机房、线路、主机等)、网络与信息安全、应用安全(应用程序的运行、数据库等的安全)等,当出现重大问题时应立即启动应急处置方案,做到保障不中断,功能不失效。只有通过建立有效、规范的应急处置预案,才能应对各种可能出现的突发情况,并防患于未然。

## 4 军校教学保障管理系统实例

军校教学保障管理系统是一套保障管理信息化的软件系统。

### 4.1 系统的内容

军校教学保障管理系统立足于军事训练综合信息网内的学院园区网。主要包括四个模块:教保处(科)、教育技术中心、图书馆、装备处(科)。从设备、场地(所)、教材(电视教材)、文具、阅览室、网站资源等方面收集存储信息。重点教学部位加入远程视频,实现远程导调。该系统使用 B/S 技术,采用 SQL 数据库,利用 JSP 和 .NET 等先进平台开发制作。用分级密码管理用户,实现各部门信

息的共享。主要流程如图 1 所示。

4.2 系统的主要功能

- 1) 以校园网为平台，实时收集、动态显示、精确统计院校教学保障管理信息。
- 2) 首长通过本系统可以准确掌握教学保障情况（如场地教学楼使用、教材使用与库存情况、阅

- 览室的使用、装备库存等），通过远程视频可以直视教学现场，身临其境。
- 3) 对于重点教学现场生成教学视频，存入网络教学资源库，加强网络教学。
- 4) 利用数据挖掘技术，对大量教学保障信息进行科学处理，进一步优化教学保障方案，为合理投入保障经费提供领导决策。

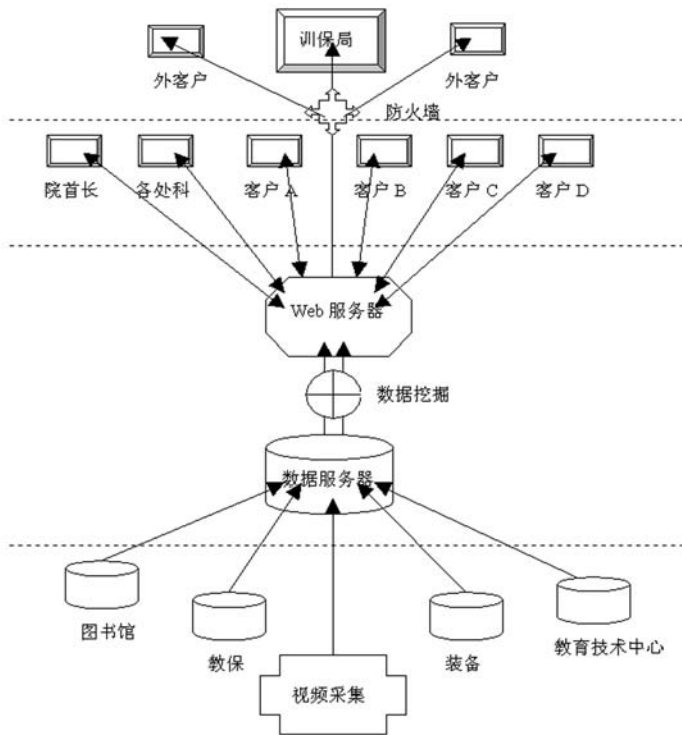


图 1 军校教学保障管理系统

参考文献

[1] 《军队院校教育信息化基础研究》 陈云昌等主编. 北京：国防大学出版社 2005.11.1

[2] 《军校教育信息化研究》 车先明主编. 北京：解放军出版社 2005.1.1

[3] 《军校教育信息化研究》 吕云峰编著. 北京：解放军出版社 2006.3.1

作者联系方式

通信地址：江苏徐州工程兵指挥学院教育技术中心  
邮政编码：221004  
联系电话：1590521849

# 基于软构件的军事信息系统的设计与实现

王揽月 平刚 全洪亮

**摘 要:** 基于软构件技术的开发模式是软件工程化开发的必然趋势。本文首先对软构件技术进行了介绍, 然后结合军事信息系统的研制开发, 讨论了软构件的设计与组装, 最后提出了目前使用软构件开发系统所面临的问题。

**关键词:** 软构件; 分布式; 设计与实现

## 1 引言

我军信息化建设如火如荼, 正朝着一体化方向发展, 其精髓之一就是软件构件化、模块化, 目的是提高软件的可重用性, 实现各系统间的互通互操作。军事信息系统是我军信息化建设的一个重要的组成部分, 军事信息系统应用于各级指挥所, 完成相关信息的收集、传递、处理与分发, 为军事管理工作提供先进可靠的信息化支持手段。为完成各级军事信息系统间的互通互操作, 各指挥所需采用通用和共用的软件构件, 基于软构件的军事信息系统研发具有重要的现实意义。

## 2 软构件技术

软件行业的工业化趋势导致了软构件的产生。能够像硬件系统那样, 将部分软件组合起来构建软件系统, 一直是软件行业多年来追求的目标。能结合系统的实际情况充分利用已有的软件构件并进行有效重组和集成, 将会大大提高生产效率, 减少大量的重复劳动, 为此, 人们提出了基于软构件的软件开发方法。和传统的软件开发方法相比, 软构件的开发方法把构架清晰地从系统逻辑中隔离出来, 便于分析较为复杂的系统, 组织规模较大的开发, 并降低系统的开发成本。

软构件技术是基于面向对象的, 以嵌入后马上可以使用的即插即用型软构件概念为中心, 通过构件的组合来建立应用的技术体系。软构件又称构件、元件, 是可复用的软件组成成分, 可被用来构造其他软件。它可以是被封装的对象类、类树、功能模块、软件框架、软件构架(或体系结构)、文

档、分析件、设计模式等, 具有如下特点: 遵循统一的标准, 支持即插即用; 支持对象意义上的封装、多态和继承; 外界只能通过接口进行访问; 它是一个支持互操作的对象, 可以在跨地址空间、网络、语言和操作系统的异构环境下被调用, 与其他软构件组装在一起协调工作。

软构件技术应用于军事信息系统, 是通过构件组合支持应用的开发环境和系统总称, 研究的主要内容包括: 构件获取、构件模型、构件描述语言、构件分类及检索、构件组装和标准化等。软构件具有类似硬件芯片的性质, 即它的结构和功能被封装在构件内部, 每个构件都有接口, 并通过接口与外部相连。构件类对应于对象中的类, 但生成实例时可以采用各种灵活的手段, 如宏定义、变异、环境设置变量等, 也可以采用动态链接与嵌入的方式。构件的种类较多, 除基本构件和领域构件外, 还包括有构架、体系结构、参考模型、设计件、中间件、分析件等。

## 3 系统设计与实现

通过对软构件技术的研究, 我们采用一种新的开发方法——积木法来开发军事信息系统。采用积木法开发系统的过程与搭积木的过程很类似, 首先构筑系统的总体框架, 然后构造各个构件, 并依次把构件安装到系统中去。软构件系统结构见图 1。军事信息系统通常包含若干子系统等, 而大部分子系统, 在功能上有类似之处, 因而利用软件的重用技术就可以把开发过程大大简化。积木法的采用正是基于这种设想。

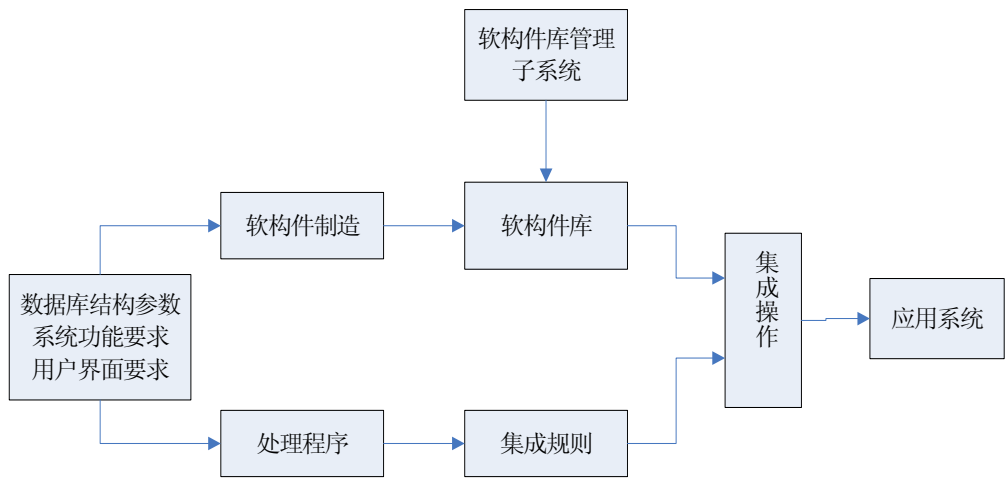


图 1 软构件系统结构

3.1 系统体系结构

二层客户机/服务器体系结构的分布式系统的组合和集成能力有限，而三层客户/服务器体系结构可以解决这一问题。大型军事信息系统可采用三层结构，即：底层为数据层，由数据服务器组成，提供数据库服务，还可提供诸如文件系统，数据仓库等数据的管理；中间层为应用层，实现系统中的关键业务处理，如构件库管理、构件分发服务等；外层为用户层，直接为用户服务。采用三层的客户/服务器结构，基于软构件技术开发应用系统，以适应系统功能扩展和领域软构件更新的需要。

3.2 软构件的设计与开发

系统生成是建立在一个个积木块——软构件的基础之上的。积木法在确定系统总体框架、构筑总体框架、修改总体框架、构造构件以及修改构件等阶段，都同一个叫做“软构件集合”的实体打交道，这个软构件集合也被称为“软构件库”。在开发系统之初就应该着手准备这个软构件集合，开发系统的大部分工作都集中在构造软构件阶段。这一阶段的工作特点是尽量使开发出的积木块具有较大的灵活性和变通性，为重用作好准备。每开发出一个积木块，都要把该积木块及其功能、调用接口等信息放入软构件集合。

我们可以按多个侧面对构件进行分类：

按开发过程构件我们将软构件分为程序件和数据件。按功能分，分为三层：基础层为基本数据类构件和系统支撑构件；中间层为各种通用的中间

件；顶层为针对业务领域的专用构件或子系统构件。从粒度上看底层的粒度较小，而顶层的粒度较大。每个程序件都应具有相同的封装形式，以便于软构件的组装和分发。数据件也是一样。

3.3 软构件的组装

采用软构件技术开发系统的设计目标是以积木组合开放式结构构造集成一体化的环境。采用积木法的关键就是要借助对积木构件的重用组合技术，进行构件组装，利用现有构件组装成新的系统。构件的组装按其特征分为黑盒组装方法、白盒组装方法和灰盒组装方法，其划分的依据是构件组装时需要了解构件内部细节的程度。其中黑盒组装方法是最理想的方法，在组装时不需要对构件的实现细节有任何的了解，也不需要对其进行配置进行修改。各个软构件开发完成后，就可以组装了。我们通常按黑盒组装方式，用应用系统组装工具来组装各子系统，通过该工具按需从构件库中选取适当的构件或典型配置搭建新的应用系统，生成系统段。在组装过程中可直接预览系统的运行总体界面，实现“所见即所得”的系统构成目标。

3.4 软件的部署

组装完成后生成每个子系统的系统段，剩下的步骤，就是要把我们的系统以及各个软构件部署到客户机上。整个软件的部署可以通过直接部署系统段的形式实现，也可以进行单个软构件的部署。部署顺序通常是先数据件，后程序件。我们通过软件

分发工具可以将组装完成的系统段分发给相应台位，完成软件的部署。

## 4 结束语

具有分散和联合处理能力的开放性分布式软构件技术的目标是实现开放的软构件产品，使应用程序能相互操作，降低开发与管理费用。通过某军事信息系统开发我们发现，在大型软构件库的支持下，利用现有的、质量好、可靠性强的软构件，按照大规模软件开发的工程规范进行开发，可以满足建设大型军事信息系统的要求，各种技术形成的软构件可以较大程度地进行重用，提高了开发效率，

降低了开发成本。

目前我们在使用软构件技术进行军事信息系统建设时还面临着一些问题，比如：领域构件粒度过大，不利于软件的复用；缺乏对用户提交的构件进行审核的机制，使构件的正确性难以得到保证；缺乏对构件使用的跟踪机制，很难确定某一构件的流向和应用情况。如何有目的的生产构件和从已有系统中挖掘提取构件；如何建造面向对象的软构件库结构，并有效地对软构件进行组织和管理；如何发现构件之间的交互错误以及集成框架与构件间的交互错误，达到集成测试构件化软件的目的等，都是亟待我们研究和解决的问题。

## 参考文献

- [1] 张凌晓，袁东锋，基于软构件的考试系统的设计与实现，计算机系统应用，2007，8
- [2] 周晓峰，王志坚，二进制构件柔性组装机制及其形式化研究，计算机工程，2006，11
- [3] 杜建伟，顾斌，基于流程的构件库管理系统及其实现，计算机系统应用，2007，8
- [4] 张毅坤，叶涛，邢传玉。面向构件化软件的合约检查测试框架，计算机工程，2006，10

## 作者联系方式

通信地址：北京市海淀区万寿路3号91655部队

邮政编码：100036

联系电话：010-66974132

# 军事信息资源目录体系初探

王锐华 张利锋

**摘 要:** 本文在研究了军事信息资源目录体系的需求和概念的基础上,对军事信息资源目录体系建设方案以及相关的政策法规制定进行了初步探讨。

**关键词:** 军事; 信息资源; 目录体系

## 1 需求分析

军事信息资源是指军事部门或者为军事部门采集、加工、使用、处理的信息资源,它产生于军事活动的各个环节和部门,存在和分布于多个领域、多个部门、多个地域。军事信息资源的有效开发和利用,对促进我军信息化建设起着至关重要的作用。由于目前相关机构分权管理,军事信息资源储存地点分散、搜寻不易。为了实现军事信息资源的共享,需要一种可分可合的工具来管理各类信息资源;需要依据信息属性对信息资源进行采集、分类、加工处理和存储,实现信息资源的有序组织;需要提供一种支持有权用户检索、定位、获取和使用信息资源的工具,满足用户在大量信息资源中准确、全面、迅速、方便、经济地获取所需信息内容的各种要求。军事信息资源目录体系是解决上述需求的有效工具。

## 2 概念内涵

对军事信息资源目录体系的理解应建立在以下几个概念之上。

### ● 目录

目录是按次序编排以供查询的信息资源的名目,例如图书目录是图书或篇章的名目,是揭示、识别和检索馆藏文献的工具。图书馆目录体系是指图书馆所确立的目录种类及其相互补充、相互联系的有机整体。

### ● 信息组织

信息组织是对所采集的信息资源实施序化的过程。

### ● 元数据

元数据是数据的数据(Metadata),它从信息内容、载体形态、信息资源集合及其组织体系、管理与服务机制以及过程与系统等方面去描述信息资源的特征和属性。借助元数据,人们可以采集、组织、识别、定位、发现、评估和选择信息资源,实现简单高效地检索、交换、管理海量数字化信息资源。运用 XML 标识语言,通过元数据与分类表、主题词表的结合,可以方便地按应用需要组织信息资源分类目录、主题目录和其他目录,实现对数字资源的导航、检索、定位和交换服务。

根据目录、信息组织、元数据等相关概念,可以从技术角度定义军事信息资源目录体系为:

以元数据为核心,以业务分类表和主题词表为控制词表,对军事信息资源进行网状组织,满足从分类、主题、应用等多个角度对信息资源进行管理、识别、定位、发现、评估与选择的工具,可为信息资源使用者或应用系统提供军事信息资源的发现和定位服务。

对军事信息资源进行编目,生成军事信息资源目录内容时,军事信息资源目录体系应该有统一的标准和规范,达到管理军事信息资源,实现军事信息资源共享的目的。

## 3 国内外研究现状

对军事信息资源目录体系的研究可以借鉴其他信息资源管理方法。

美国等发达国家从 20 世纪 70~80 年代就开始研究和出台了一系列管理政策对政府信息资源进行管理,如《文书工作缩减法》和《政府信息资源管理政策》。为了整合政府的公共性信息资源,为公众提供单一窗口的政府信息导航、检索与定位服务,1994 年 12 月美国商务部将政府信息定位服务

GILS 计划作为联邦政府信息处理标准 (FIPS 192) 颁发, 公布正式建立 GILS。此公告并要求所有政府单位机构必须在 1995 年 12 月 31 日前实行 GILS 检索系统的使用。美国 NIST (国家标准暨技术局) 规定所有联邦机构必须采用 GILS 来定位文件出处。1995 年起, 美国将 GILS 作为政府信息基础设施的核心组成部分进行建设。

近几年, 随着信息化建设的不断发展, 为了合理开发、有效管理和充分利用信息资源, 我国在政务信息资源、文化信息资源、科技信息资源、交通信息资源、自然资源和地理空间等不同领域, 不同程度地开展了信息资源共享和交换的研究和建设, 分别建立了各自的信息资源目录体系和交换体系, 以支持跨部门、跨地区、跨领域信息资源的共享和交换。

## 4 建设建议

军事信息资源目录体系建设是军队信息化的必经之路, 是在今后需要长期坚持, 细致开展的一项复杂工作。它涉及的范围广、部门多, 需要遵循和制定与之配套的一系列方针政策、管理制度、法律法规、标准规范。建议从以下几方面开展目录体系的建设。

### 4.1 加强认识、统一规划

目前我军对军事信息资源建设的重要性有了一定的认识, 但是对军事信息资源共享和交流的认识还不够, 因此军事信息资源目录体系建设的首要任务是加强对军事信息资源共享重要性的认识。

由于军事信息资源的开发涉及的部门、地域繁多, 必须由总部机关整体规划军事信息资源开发利用总体框架, 在统一的框架下进行开发建设, 总体协调军事信息资源的开发内容和步骤, 避免产生新的问题; 要明确军事信息资源管理权限的纵横分配, 界定军事各职能部门的信息资源管理范围和职责, 明确与其职能相关的信息资源目录制作的权利和义务, 才能有利于信息资源的长期开发、维护、管理和利用, 达到可持续发展的目的。

### 4.2 制定政策、建立制度

在军事信息资源开发利用中, 首先应该针对军

队的信息资源管理制定相关政策, 尽快研究和制定出军事信息资源管理规程。从军事信息资源管理总则、管理体制、信息主体的权利和义务、军事信息资源开发和利用的政策规范、共享机制、安全保护、版权管理、法律责任和数字信息资源保存本身等方面规范军事信息资源的开发利用行为, 为信息资源开发和利用构造一个良好的政策环境。

建设军事信息资源目录体系需要有相关的管理制度配套, 只有在一定的管理制度规范下, 才能建成军事信息资源目录。需要制定的相关配套制度有:

- 建立信息资源采集、组织、分类、保存、交换、发布与服务管理制度
- 建立军事信息资源分级联合编目、申报与登记制度
- 建立军事信息资源元数据标准申报登记备案制度
- 军事信息资源唯一标识 (编码) 申请、分配制度

### 4.3 研究标准、规范框架

军事信息资源目录体系建设标准规范必须先行。需要围绕信息采集、组织、分类、保存、发布与使用等信息生命周期各环节建立规范和标准。主要有以下几方面。

#### (1) 研究和出台信息资源元数据标准体系

军事信息资源元数据标准体系包括: 技术标准、信息组织标准和控制词表标准。我国建设军事信息资源目录体系的当务之急是参考国际标准, 尽快研究和出台我军信息资源元数据、分类标准、唯一标识编码标准、目录制作技术标准等, 为我军军事信息资源目录体系建设提供基础。

#### (2) 规范和出台信息资源分类标准框架体系

确定军事信息资源分类的总体框架以及分类原则。如按行政结构、公开与保密、信息属性、机制、来源、服务对象等, 研究和设计军事信息资源的根分类; 各领域具体的信息分类方法可参考各领域已有的分类法; 还可根据具体的使用目的按地域、体系、学科、主题、应用等分类。

#### 3) 军事信息资源目录的管理与存储模式

由于军事信息资源的存在和分布是多专业、多部门、多地域的, 从军事信息资源的建设、更新、管理维护、利用、版权管理和信息安全等方面考



虑,不宜采用完全集中式的管理和存储办法。建议军事信息资源按总部机关、专业、地区分布式管理与存储。

军事信息资源目录应采用集中分布式管理与存储,在政务外网平台存储和提供军事信息资源总目录,行业与地方存储和提供行业或地方相关军事信

息资源分目录,也可与军事信息资源总目录定时同步,提供基于总目录的导航服务。

在上述工作的基础上,建议选择有代表性的部门首先进行信息资源目录体系的试点建设,发现问题,总结经验,不断完善,最终向全军推广。

### 参考文献

- [1] 高复先,吴曙光等编译,信息工程于总体数据规划,人民交通出版社,1989
- [2] 高复先,信息工程开发工具的研究,中国计算机报,1994年第1期
- [3] 高复先,信息系统集成与国民经济信息化,工程设计CAD及自动化,1995年第5期
- [4] 孟广均,沈英等,信息资源管理导论,科学出版社,2000
- [5] 钟守真,李培等,信息资源管理概论,南开大学出版社,2000
- [6] 杨学山,企业信息化建设和管理,北京出版社,2001
- [7] 高复先,信息资源规划—信息化建设基础工程,清华大学出版社,2002.4
- [8] James A.Senn. Information Systems in Management (Third Edition).Wadsworth Publishing Company, Inc., 1978
- [9] J ames Martin and Clive Finkelstein. Information Engineering. Prentice-Hall, Inc., 1981
- [10] William Durell. DATA ADMINIDTRAION ----A Practical Guide to Successful Data Management. cGraw Hill, Inc.,1985
- [11] Andrew S Targowki. Managing Information Through System Architecture—The systems Logic Integration Approach, Information Executive. The Journal of Information Systems, Vol 3 No.3 Summer 1990
- [12] Mar Humphries, Michael W.Hawking, Michelle C.Dy. DATA WAREHOUSEING Architecture and Implementation. Prentice Hall PTR, 1999

### 作者联系方式

通信地址:北京市丰台区大成路13号Z01

邮政编码:100039

联系电话:010-66820128

# 做好国防信息化评估，提升国防信息化建设水平

王顺满 许楷

**摘 要：**国防信息化评估是国防信息化建设的重要方面，通过评估工作能够找出信息化建设的差距，分析存在的问题并提高国防信息化建设水平。而国防信息化建设作为一个复杂系统，对其水平的评估之关键在于给出适合国防信息化建设约束条件的评估指标体系与评估方法。本文分析了国防信息化建设的相关背景知识，从国防信息化评估的必要性，指标体系，评估方法等方面提出实施国防信息化评估的建议。

**关键词：**国防信息化；评估；复杂系统；对策建议

## 1 序言

“信息化”是一个舶来语，最先出现在 20 世纪 60 年代日本学者的《论信息产业》一文。目前，信息化仍是一个动态发展的概念，其所强调的主要是从一种状态到另外一种状态的变化过程。信息化水平已成为 21 世纪衡量一个国家或地区经济发展程度和竞争实力的重要标志。目前，世界上的发达国家都在竞相发展和提高信息技术水平，大力发展信息产业，以尽快提高国家信息能力，从而提高国家综合国力，以便在 21 世纪的竞争中处于领先地位。国防信息化作为国家信息化建设的重要组成部分，对于保证国家安全与领土完整以及维护国家利益等方面起着重要作用。信息化战争将成为 21 世纪战争的主要形态，所以必须要以信息化建设为国防建设与信息化建设的主要目标。我国国防体系的机械化建设任务还没有完成，同时又面临着信息化的严峻挑战，处理好机械化与信息化的关系，关系到国防和军队现代化建设长远目标的实现。如果按部就班，在完成机械化建设任务后再进行信息化建设，就会错失良机，无法赶上西方发达国家的建设步伐；如果放弃机械化建设，把建设重点全面转向信息化，也不符合国情军情，还可能欲速则不达。就国防信息化建设来讲，其属于一个复杂巨系统，不仅有硬件设施的建设，同时还有人力资源、政策法规等软环境等方面内容。对国防信息化建设水平及其信息技术的应用环境进行评估，能更有利于了解国防体系在信息社会进程中的迈进程度，找出信息化建设的差距，分析存在的问题并通过相应的发展策略与实施促使来提高国防信息化的建设水平。

## 2 国防信息化及进行国防信息化评估的必要性

### 2.1 国防信息化的典型特征

国防信息化建设的本质是以提高信息力为根本目的，以“系统集成”为主要途径，最终把以物质和能量为国防力量战斗力核心构成要素的、适于打机械化战争的机械化国防力量，建设成以信息技术为国防力量战斗力核心构成要素的、适于打信息化战争的信息化国防力量的过程，我国的国防信息化具有如下特征。

首先是国防信息化建设的时代性，即国防信息化建设出现于由工业社会向信息社会的转型期，它是随着信息时代来临的一个必然产物。

其次是国防信息化建设的目的性，即要求改变工业时代围绕提高火力和机动力建设国防力量的旧观念，树立以提高国防力量信息力特别是信息防护能力为中心的国防建设思想，最终实现以信息力为国防力量的主导性作战能力构成要素。

第三，实现国防信息化建设的主要途径是“综合集成”，建成以军事信息系统为龙头的信息化武器装备体系，然后实现预警探测、指挥控制、精确火力打击等功能于一体，实现信息化军队和信息化后备力量的一体化，最终把整个国防力量建设成结构和职能一体化的国防大系统。

第四是要适于打信息化战争，这就要求国防信息化建设要以信息化战争理论为牵引，按照打赢高技术战争特别是信息化战争的要求，大力发展信息化武器装备，建设信息化后备力量和信息化国防动

员体制,积极培养新型高素质国防信息化建设人才。

## 2.2 国防信息化评估的重要意义

国防信息化建设评估体系对于准确把握我国国防体系建设现状,分析存在的问题,找出存在的差距,并提升我国国防体系信息化建设水平具有重要意义。

首先,国防信息化建设评估是指从定量角度来评价国防信息系统及其环境的现状、水平和发展潜力,反映国防信息化的程度与进度。准确、客观地对国防信息化进行评估是国防信息化建设的一项重要任务。国防信息化建设涉及资源、装备、技术、人力、政策、环境等诸多方面。因此,进行国防信息化评估时,需要根据国防信息系统的特点,结合时空变化,从不同的层次和角度,建立一整套量化指标体系,进而对国防信息化进行准确、客观的定量评估。

其次,国防信息化水平标志着一个国家国防现代化的新一轮刻度。国防现代化进程中,我们迫切需要了解我国国防信息化的发展状况、信息化水平、信息化对国防建设的影响与军事强国国防信息化的比较以及在世界上所处的位置等问题。这就要求我们必须尽快建立科学合理的、适合中国国情的国防信息化评估指标体系。

第三,对国防信息化进行评估,不单是对当前的国防信息化水平有所了解,更主要的在于:通过评估在宏观上正确引导和促进我国国防信息化快速、健康发展;通过评估为我国国防信息化的规划工作提供量化的依据,做到心中有数;通过评估了解我国国防信息化建设的薄弱环节,从而弄清进行国防信息化建设应该重点从哪些方面入手,做到有的放矢。这就需要建立一套科学的国防信息化评估指标体系。

## 3 国内外信息化评估体系现状

### 3.1 哈佛大学与世界经济论坛“网络化准备指数”评估体系

2002年,哈佛大学国际发展中心与世界经济论坛合作,在基于各国信息与通信技术(ICTs)的应用现状和发展潜力的基础上,首次对世界上 75

个国家或地区网络化准备情况进行了综合评估和对比分析,并于2002年2月4日发表了题为《全球信息技术报告 2001~2002:准备进入网络世界》的研究报告,该报告以“网络化准备指数”(Networked Readiness Index)的形式公布了评估结果,为商业行动和政府政策制定提供参考。

### 3.2 美国国际数据公司(IDC)“信息社会指数”评估体系

自1996年开始,IDC每年都对全球55个国家(或地区)参与信息社会的能力进行综合评估,并以“信息社会指数”(Information Society Index)的形式公布评估结果。根据各国信息社会指数将参评国家的发展状况分为漫步型、小跑型、快跑型、速滑型4个发展等级,并从全球角度对信息化社会建设进行了分析,为处于不同发展阶段的国家提出了相关的发展建议。

### 3.3 澳大利亚“信息经济办公室指数”评估体系

澳大利亚国家信息经济办公室分别于2002年4月和2003年8月公布了一些国家的信息经济发展水平指数。根据各国信息经济的规模、发展状况和发展潜力的相关数据,NOIE进行了综合评估和对比分析,并以澳大利亚“国家信息经济办公室指数”(NOIE Index)的形式公布了评估结果,为各国信息经济建设投资提供参考。

### 3.4 英国电子经济评估体系

2002年3月,应英国信息时代联盟(IAP)的邀请,美国咨询顾问公司驻伦敦办事处与英国电子专员办公室和INSEAD商学院合作,制定了电子经济评估体系,并对七国集团成员国以及澳大利亚和瑞典电子经济的发展情况进行了综合评估和对比分析,并于2002年11月在《国际电子经济对比:世界最有效的电子经济政策》报告中公布了评估结果。

### 3.5 俄罗斯联邦各地区信息化建设评估指标体系

为了对国家和地方自治权利机构在向公民和经济实体提供服务时信息通信技术的使用情况进行检

查，并建立一套针对国家和地方自治权利机构的信息通信技术应用的指标体系和有效评估的方法，俄罗斯联邦政府于 2002 年 9 月开始对全国 89 个联邦主体的信息化建设进行评估。本次评估由俄罗斯联邦经济发展和贸易部组织，由俄罗斯网络传媒和信息技术领域的龙头企业康萨基格商务控股公司具体负责承办。

3.6 韩国“信息化指数”评估体系

韩国“信息化指数”评估体系是由韩国电算院组织制定并实施评估的。自 1995 年起，韩国电算院开始对世界上 50 个国家（或地区）的信息化程度进行评估和比较分析，并每年以“信息化指数”（Informatization Index）的方式公布其评估结果。

3.7 中国国家信息化指数（NIQ）

2001 年 7 月 29 日，原国家计委、原国家经贸委、国家统计局、国家质监局、国家广电总局、信息产业部、国务院新闻办等部门联合发布国家信息化指标构成方案。国家信息化指标的研究被业内人士称为“中国新的现代化标准”，它是全球第一个由国家制定的国家信息化标准。2002 年 3 月 19 日，国家信息化测评中心公布了国家信息化水平报告，对 1998~2000 年的国家信息化指数（NIQ）进行了权威描述。

4 国防信息化评估指标体系框架与方法

按照国家信息化建设的六要素（信息资源、信息网络、信息技术与应用、信息产业、信息化人才、信息化政策法规），参照美国关于信息化的划分，这里将我国国防信息化水平评价体系分成国防信息化的基础环境水平评估与国防信息化的社会环境水平评估两部分。在国防信息化的基础环境水平评估中主要包括国防信息化资源开发水平、国防信息化网络建设程度、国防装备信息化程度、国防信息技术应用技术程度与国防信息安全与攻防能力水平等 5 方面。国防信息化的社会环境水平包括国防信息化政策法规、国防信息化人才建设情况和国防信息化软环境建设情况等 3 部分。其结构如图 1 所示。

在对国防信息化水平进行评估时，可以采用理论分析、经验选取和专家咨询相结合等不同方法，

具体使用过程中要根据实际情况进行调整。同时，对 8 项分指标的水平评估还要有一系列子指标来衡量，8 项分指标的评估要进一步细化，并要做到具体化，明确化，避免产生歧义与标准不统一等问题的出现，并要对这些子指标给出不同的权重，各个分指标的数值是在现实的资料库或数据库中可直接或间接地得到。在具体的实施过程中可以通过数值法给出国防信息化建设水平的分数表示；也可以通过分类法，根据国防信息化建设的水平将其分为不同的类别，对国防信息化建设水平的准确评估能够为国防信息化建设的健康发展起到重要的作用。

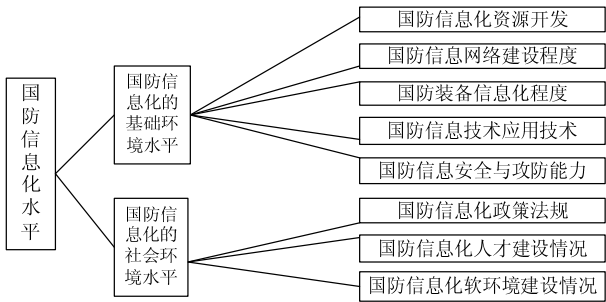


图 1 国防信息化评估指标体系示意图

5 国防信息化典型评估方法及实施过程中应当关注的问题

5.1 国防信息化典型评估方法

5.1.1 单指标评估方法

为了刻画国防信息化水平的本质特征，我们利用功效函数来计算单项指标的评估值。即首先设定一段时间内指标的最大、最小值，分别用  $\alpha$  和  $\beta$  来表示，则指标变量  $C_{ij}$  对准则  $B_i$  的功效函数可定义为：

$$C_{ij} = \frac{C_{ij} - \beta}{\alpha - \beta} \tag{1}$$

其中， $i=1, 2, \dots, 7$ ； $j$  为准则  $i$  的指标个数。

关于临界水平  $\alpha$ 、 $\beta$  的确定方法，我们采用计划期内的发展目标、历史上的最低水平确定，并结合专家意见进行修正。

5.1.2 多准则评估方法

为了测度国防信息化水平，我们利用综合评分分析法来计算各个准则的评估值。即对每一个单项指标的评估值（功效）配以权重系数（或减称权重） $W_{ij}$ ，则各个准则的评估值  $B_i$  可表示为

$$IB_i = \sum_{j=1}^n (W_{ij} \times C_{ij}) \quad (2)$$

其中,  $W_{ij}$  为指标  $C_{ij}$  的权重系数, 且  $\sum_{j=1}^n W_{ij} = 1$ ;  $n$  为  $j$  的上限。

权重系数  $W_{ij}$  的确定, 通常采用层次分析法 (AHP)。AHP 法是针对上一层次某准则, 本层次与之有关因素之间相互比较, 构造出判断矩阵, 然后通过特征值法求出相对权系数。

### 5.1.3 信息化的总评估方法

#### (1) 线性加权求和法

线性加权求和法是最为常用的建立评估模型的方法, 它具有简便、易懂等优点。其基本思想是: 将各个评估准则对被评估目标的贡献之和作为被评估目标的评估值。评估准则对被评估目标的贡献, 等于该评估准则对被评估目标的贡献率 (即该评估准则的权重系数) 与该项评估准则的得分的乘积。其数学表达式为

$$H = \sum_{i=1}^7 (W_i \times IB_i) \quad (3)$$

其中,  $H$  为国防信息化水平总指数 (Informatization Index);  $W_i$  为各个评估准则的权重系数, 且  $\sum_{i=1}^7 W_i = 1$ ;  $IB_i$  为第  $i$  个评估准则  $B_i$  的得分 (即评估准则  $B_i$  的评估值)。

将式 (2) 和式 (3) 合并, 可得

$$H = \sum_{i=1}^7 W_i \times \sum_{j=1}^n (W_{ij} \times C_{ij}) \quad (4)$$

#### (2) 指标乘积法

国防信息化水平的评估值由各单项指标加权求和而得, 这表示它们之间是可以互相代替的。而事实上, 衡量国防信息化水平的有些指标是不可或缺的, 它们之间不能互相替代, 加权求法对此不适用。如用百分制进行评估, 若信息安全能力的权重是 0.2, 这样即使信息安全能力为 0 分, 其他六项相加仍可得 80 分, 总成绩还是良好水平, 这显然不符合国防信息化全面建设的要求。

针对这一情况, 可以运用指标乘积法, 即以指标间相乘代替相加, 反映其不可或缺的关系, 从而建立一个立体的全方位的评估模型, 其数学表达式为

参考文献 (略)

作者联系方式

通信地址: 北京市 2518 信箱

邮政编码: 100041

联系电话: 010-68893627

$$H = \sum_{i=1}^7 IB_i^{W_i} \quad (5)$$

将式 (2) 和式 (5) 合并, 可以得到:

$$H = \sum_{i=1}^7 \left( \sum_{j=1}^n (W_{ij} \times C_{ij}) \right)^{W_i} \quad (6)$$

## 5.2 国防信息化评估应注意的问题

国防信息化建设是由软硬件环境组成的一个复杂巨系统, 由于多种因素的共同限制, 制定一种科学、合理的信息化评估体系确实存在一定难度。由于国防信息化建设的特殊性, 我们认为在制定国防信息化评估方案时应当注意如下几方面问题:

首先, 在制定国防信息化评估方案时要考虑结合本国的实际情况。在此基础上, 还应当对现有国际上典型的信息化建设水平评估体系进行研究, 借鉴国外好的方案。尽可能地覆盖各种体现信息化水平的要素, 以增强评估体系的可操作性、可比性和导向性。

第二, 由于信息技术与武器装备的发展日新月异, 其普及应用的广度和深度不断加大, 已经出台的信息化评估体系也需要根据实际情况及时做出相应的调整。

第三, 在进行具体评估时, 要特别注意评价指标的确定性与含义明确性。针对不同应用背景要给出比较普适的评估方案。同时在实施过程中应当以第三方评估, 以做到客观、科学, 真正反映出存在的问题与取得的成绩, 以为更加系统地国防信息化建设提供依据。

## 6 结束语

国防信息化建设对于新军事变革起到重要影响, 是新军事变革的核心。在进行国防信息化建设的过程中要特别关注建设情况的评估。通过评估工作来交接国防信息化建设的现状并分析存在的问题, 找出下一步建设的重点。其对国防信息化建设影响至关重要。而在评估过程中应当特别关注评估指标的选取与评估方法的确定, 并在实际操作过程中针对不同情况给出适当调整以更为有效地提出应对措施, 提升国防信息化建设水平。

# 军事装备全寿命信息管理研究

王增 徐启建

**摘要:** 随着现代军事装备的快速发展和技术复杂程度的增加,在装备信息资料的管理和利用上面临许多困难,而信息技术的飞速发展为实施装备全寿命信息管理带来了转机。本文简要分析了目前我军在装备信息资料管理中存在的主要问题,阐明了装备全寿命信息管理的概念,对美军全寿命信息管理的历程及其主要做法进行了介绍,对我军实施装备全寿命信息管理面临的技术挑战进行了探讨,最后对我军实施装备全寿命管理提出了发展建议。

**关键词:** 军事装备;全寿命信息管理

## 1 引言

装备全寿命管理是指对装备从计划立项、研制生产、部署使用直到退役的全过程管理。对于庞大复杂的军事装备,在装备全寿命过程的各个阶段会产生大量的技术数据和管理数据,以及各种活动所产生的原始数据和不断更改的动态数据信息,这些数据信息数量巨大且种类、格式繁多。长久以来,我军装备数据资料主要以书面纸张等物理形式存在,因此如何解决这些数据资料所带来的维护费用过高、修改困难、体积与重量过大、交付与传递及时性差,容易产生重复、冗余数据,安全性难以保障,以及不能满足各种计算机辅助技术对数字技术数据的需求等问题,是摆在我们面前的一个重大课题。信息技术的发展给我们带来的前所未有的机遇,装备全寿命信息管理势在必行。

## 2 装备全寿命信息管理的基本概念

全寿命信息管理是在军队和国防工业系统范围内采用统一的标准将装备研制、生产与使用保障过程中的技术数据与事务数据数字化并开发信息系统,用数字形式的数据进行交换、存储、联机服务与管理,为装备全系统、全寿命管理提供集成数据环境。装备全寿命管理的主要目标是从装备信息无纸化入手,最终建立集成数据环境,实现装备全寿命过程信息的数字化、自动化、网络化与集成化。

## 3 外军全寿命信息管理研究

研究和推进装备全寿命信息管理对于我国和我军来说,是一个新的课题,学习和借鉴发达国家的实践经验是非常必要且有益的。实际上,我国所称之的“全寿命信息管理”,即为在美国及其他西方国家所普遍使用的“CALS”。

### 3.1 CALS的发展历程及内涵

随着信息技术的发展及武器装备采购需求的牵引,CALS 的内涵、应用范围及技术手段在不断拓展,其名称经历了 3 次修改:

(1) 计算机辅助后勤保障 (Computer Aided Logistic Support)

它是美国国防部 1985 年 9 月提出的一项战略计划,旨在利用计算机技术将人工的、以纸张为载体的技术文件密集型工作方式转变为高度自动化与集成化的工作方式,以数字化方式管理军事装备的技术资料,革新装备的后勤保障方法。

(2) 计算机辅助采购和后勤保障 (computer-aided acquisition and logistic support)

1987 年,美军在原来的名称中加入“acquisition”一词,这是因为 CALS 不仅可以解决后勤保障问题,而且可以简化军事装备的的采购程序。

(3) 连续采购与全寿命保障 (continuous acquisition and life-cycle support)

1993 年以后,CALS 的范围进一步扩大,在国

防部与国防工业界，其信息数字化的重点转移到装备的持续采办与整个寿命周期保障所产生的所有数据，除技术数据外还包括行政管理、型号管理、财务、商务等数据。扩大后的 CALS 范围，则完全适用于民用工业与企业。因此，美国国防部将 CALS 改称为“持续采办与寿命周期保障”

#### (4) 光速商务 (commerce at light speed)

克林顿政府更关注国家基础信息建设以及包含 EDI (电子数据交换) 在内的广义电子商务。因此，1994 年美军将 CALS 又赋予“光速商务”这一释义。

目前，CALS 的释义“连续采办与全寿命保障”和“光速商务”被普遍接受，我军称之为“全寿命信息管理”比较符合我国实际。

### 3.2 美军CALS的主要做法

- 1) 制定分阶段实施的 CALS 计划，明确各阶段目标；
- 2) 实行统一 CALS 的标准；
- 3) 重视信息设施基础现代化建设；
- 4) 设立专门的 CALS 管理机构，实行集中统一指导；
- 5) 在武器系统采办中实施 CALS。

## 4 我军实施装备全寿命信息管理面临的技术挑战

信息技术在为发展军事装备带来机遇的同时，也给装备的发展带来了严峻的挑战。

1) 不同商家的计算机软件和硬件，所产生的信息数据，往往不能完全兼容，缺乏互操作性，信息交换困难，给工作协调带来了很大的难度。

2) 大型军事装备系统的全寿命周期往往长达十年以上，而计算机、网络设备和软件等许多信息技术产品有时 2~3 年就更新换代。信息技术的飞速发展使得一些装备“自生至死”往往经历几代信息技术或产品的发展。如何保证在数十年后的信息技术还能读取现在计算机所产生的数据信息，这就为选用信息技术带来很大的风险。

3) 由于信息数字化，信息安全和保密要求有了新的内涵，需要对随意拷贝、病毒感染、黑客侵袭以及机器损坏而造成信息丢失或破坏等不安全因素采取多种防范措施。在装备全寿命信息管理中，信息安全保密是至关重要的头等大事。然而到目前

为止，信息安全保密在全世界都还有待进一步研究解决的重要课题。

## 5 我军实施装备全寿命管理的几点建议

装备全寿命信息管理由管理信息系统实施。进行有关装备信息收集、处理和传输的系统称为装备管理信息系统。下面，就我军装备全寿命信息管理建设及其管理信息系统建设提几点建议。

### 5.1 加强统一领导和统筹规划

装备全寿命信息管理的建设是一个由军队与国防工业系统共同参与的大型信息化工程。对于这样一项大型的信息化工程，为了能够做到统一的政策、统一的标准和统一的行动，必须建立一个高效的领导与管理机构，加强对装备全寿命信息建设的集中统一的领导，主动地领导和引导各单位的管理信息系统的开发与管理，减少浪费和低水平重复建设，防止出现“孤岛”现象。军队与国防工业系统应当按照“统筹规划，统一设计，统一标准，联合建设，互联互通，资源共享，目标共同，互利互惠”的原则，紧密配合、密切协作。

同时，应当确立统筹规划、分阶段实施的建设方针，由上而下全面地规划全军的装备全寿命信息管理建设。

### 5.2 加强国防信息基础设施建设

进行装备全寿命信息建设必须加强国防信息基础设施，要把信息基础设施作为最基本、最重要的要素摆到装备建设信息化的重要地位。遵循国家信息化建设关于“军民兼顾，专通结合”的原则，以国家信息基础设施为依托，加速国防信息网的建设。同时要汲取国外在推行信息化的早期曾走过的三军各自独立开发互相不兼容、不通用的信息平台的弯路经验教训，从装备信息统一开始建设，就应当规划开发三军统一的信息处理平台。

### 5.3 制订装备信息系统标准体系，做好标准化工作

装备全寿命必须采用统一的标准，因此，应当

制订装备全寿命信息标准体系，加强标准化工作。在制订标准体系时，除制订我军装备全寿命信息管理建设所需的法规、管理规定、数据库词典与一些专用的标准外，其他数字数据格式与数据交换、通信、计算机及中文处理等标准优先采用国际通用标准和尽量选用现有的国家标准、军用标准及军种与行业标准。

## 5.4 大力开发利用信息资源

信息资源开发利用是装备全寿命信息管理的核心的任务，也是建设工作能否取得成效的关键。这里所指的信息资源是数字形式的电子信息资源。由于历史的原因，我军信息资源的开发利用还是一个比较薄弱的环节。具体表现在：大部分装备信息还处于原始的、分散与孤立的状态和纸面的、静态的形式，没有加工整理成可交流共享的、动态的电子形式的数据库或信息系统。因此，必须大力开发利用各种装备的信息资源。

## 5.5 积极组织对实现装备全寿命信息管理的关键技术与应用的研究

组织力量对信息安全、软件智能化、系统集

成、分布式数据库与数据仓库、联机集成技术信息服务、交互式电子技术手册等关键技术及应用技术进行技术攻关。将已经取得的技术成果应用于装备信息系统建设。同时，积极开展学术交流活动，以促进装备全寿命信息管理的建设。

## 5.6 抓紧信息技术人才培养

信息化建设，人才是根本。实施装备全寿命信息管理建设需要一大批掌握最先进信息技术 的专门人才和热心于信息化建设的管理人才，因此，应当抓紧制订信息技术人才培养计划，加快人材培养，以满足装备全寿命信息管理建设的需要。

## 5.7 高度重视信息安全建设

要把信息安全提到关系国家安全和装备建设信息化建设成败的高度来考虑。为此，装备信息系统必须采取以下对策与措施：采用与国际互连网络物理隔离的专用网络，对上网传输的内部以上装备信息采取全文数据加密，开发与使用自主技术的信息安全产品，研究与综合运用安全技术、建立一套信息安全机制、强化信息安全管理。

## 参考文献

- [1] 黄栋，张怀强. 装备技术资料管理问题探讨. 中国科技信息，2005 年第 17 期
- [2] 张怀强，魏汝祥，张金龙. 武器装备全寿命信息管理研究. 海军装备 [J] 2003 年 11 月
- [3] 董长富，郭超平，王国勇. 通信装备全寿命管理理论的研究与实现. 国防技术基础 [J] 2005[10]
- [4] 花兴来，刘庆化. 装备管理工程. 北京：国防工业出版社，2002
- [5] 王汉功等. 装备全系统全寿命管理. 北京：国防工业出版社，2003

## 作者联系方式

通信地址：北京丰台区大成路 13 号 Z02

邮政编码：100039

联系电话：010—66820123



# 处置核化事件中指挥信息系统组织运用问题研究

王祖平 高峰

**摘 要：**中央军委颁发的新一代《中国人民解放军司令部工作条例》，明确规定了部队在遂行任务中要组织建立指挥信息系统，确定了部队组织指挥处置突发事件行动的具体要求。本文根据新条例界定的指挥信息系统组织建立范畴和有关规定，结合战区担负此类任务部队的实际情况，针对核、化突发事件特点及其对指挥信息系统组织运用的影响，对现阶段处置核化事件中指挥信息系统组织运用问题进行了研究，探讨了系统组织运用的具体方法，提出了系统组织运用中需要重点把握的问题。

**关键词：**处置核（化）事件；指挥信息系统；组织运用

“朝核危机”是当今全球热点问题之一，2006年朝鲜在靠近我方一侧贸然进行核试验，曾经一度使朝核问题升温，后经我国政府多方努力达成了新一轮“六方会谈”，使“朝核危机”得以缓解，并朝着有利于问题解决的方向发展，但我们仍需做好在多种领域内处置核事件的准备。同时，“日遗化武”和民用化工企业的生产事故，也时常给国民经济建设和人民生活构成严重威胁。如2005年11月13日发生的吉林石化分公司爆炸案，不仅造成了重大人员伤亡和财产损失，而且引发了重大水污染事件，给松花江沿岸上千万人民群众生活和经济建设带来了严重影响，事件还波及到邻邦国家，引起国际社会的广泛关注。因此，有必要做好处置核化事件行动的各种准备，并有针对性地研究我指挥信息系统在处置核化事件行动中的组织与运用问题。

## 1 核化事件对指挥信息系统组织运用的主要影响

部队遂行处置核化事件任务，通常主要是派遣防化分队查明放射性污染或化学污染的范围和程度，为处置行动指挥部确定采取相应的对策和防护措施提供依据；派出医疗救援队，对辐射损伤和非辐射损伤及化学污染物中毒的伤员进行处理；派出清洗队，消除人员、地面及各种物体污染的放射性物质或有害化学物质，减轻其污染程度，以避免或减少其对人员的伤害；派出安全警戒分队，严格控制污染区边界处的进出通道，防止无关人员进入而

受到伤害，警卫重要目标和区域，维护社会治安，保护国家和人民财产不受损失；派出疏散队，组织事发地区附近一定区域内的群众，向该区域远处疏散撤离等一系列具体任务。其事件的特殊性和部队行动的特点，既与战时的防核化生作战行动有所区别，也与一般抢险救灾行动大有不同。故此，在处置核化事件行动中对指挥信息系统的组织建立及其运用，也产生着许多特殊的影响，并提出了相应的具体要求，其主要表现在：

一是事件突发性较强，处置行动准备短促，要求指挥信息系统的组织建立必须快速组网展开。核化事件，往往是在人们难以预料的时刻发生，如前苏联切尔诺贝利核电站的核泄露事故和我国前不久发生的吉化爆炸案等。核化事故爆发突然、紧急、猛烈的性质，致使部队准备的时间极为短暂。从国外处置核事故和我国处置此类事件的实践中看，为迅速控制局势、减少损失，通常军队和地方各级组织都最大限度地缩短命令成文和指令传递时间，实行决策、传递、执行的快节奏联动。因此，要求指挥信息系统主管部门及其保障分队，必须能够按上级指示和核化事件的性质，迅速调整或拟定系统组织运用方案，快速向事发地区实施机动展开。

二是污染危害性很大，处置行动环境严酷，要求在指挥信息系统组织运用中必须采取有效的防护措施。核化事件发生后，由于放射性烟羽或有害化学物质的弥散，严重的污染了周围环境，不仅使空气中放射性核素或化学物质的积分浓度很高，而且有害物质在沉降过程中，各种物体表面将受到污染，致使处置环境异常严酷，给指挥信息系统的组

网开设带来许多困难。因此,其客观环境的严酷性,要求必须采取有效的防护措施,避免或尽可能减少人员、系统装备及器材的沾染。

三是影响范围非常广,处置行动指挥特殊,要求指挥信息系统的组网开设必须满足超常指挥的需求。核化事件虽然爆发于特定的时间和空间内,但在社会信息化程度越来越高的今时,其消息将迅速传播,影响范围甚广,不仅能造成经济和生命财产的巨大损失,同时,还会对公众心理和社会稳定造成严重影响,与国家的政治、经济、外交及民心息息相关,可谓“事发一处,震动全局”。为控制事态发展和做好善后工作,核化事件处置行动中的指控形式往往超出常规,如2005年11月13日,我吉化公司发生爆炸事故时,国务院和相关省委、省政府都专门派出了的处置行动领导小组,直接指挥控制事后处置行动。因此,这就要求部队在遂行任务中其指挥信息系统必须能够满足高层指挥机构垂直指挥与控制的需要。

四是情况发展变化快,处置行动随事多变,要求指挥信息系统组网运行必须具有较强的快速应变能力。部队在遂行处置核化事件中,不仅要面对其事发突然、发展快速、影响面广、瞬息多变等复杂情况,而且要根据事件的性质,接受军地双重领导与指挥,同时还要与其他参加处置行动的各种力量紧密配合,共同执行各项任务。因此,客观上要求我指挥信息系统在组网运行中,能够按事态的发展变化情况和上级要求,随时做好快速调整或重新部署的准备。

## 2 处置核化事件行动中指挥信息系统的组织与运用

部队在遂行处置核化事件任务时,通常由多种专业分队编成处置力量,主要担负辐射监测或化学污染监测、医疗救援、放射性沾染消除或化学沾染洗消、安全警戒、消防和工程抢险及公众的疏散撤离等具体任务。在处置核化事件行动中,建立反应灵敏、精干高效、手段多样、稳定可靠的处置行动指挥信息系统,是确保处置行动指挥顺畅的重要保证。在系统组网开设时,要针对核化事件对指挥信息系统组织运用的主要影响,以及事件的性质和发展变化等情况,区分“沾染区内”与“沾染区外”的不同特点,立足以机动和便携式指挥、侦察、通

信装备为主,审慎、机动地组织实施。

### 2.1 “沾染区内”的组织

“沾染区内”是事发的重灾区,周围环境到处都存在着放射性污染物或化学污染物,对我人员和指挥、侦察、通信装备构成严重威胁。因此,对于系统集成度高、综合要素多、结构组成复杂的大型指挥信息系统装备切不可进入,以免事后因难以洗消而导致装备废置。这就要求首先应把“沾染区内”需要组织建立的网系,定位在指挥信息系统的“末端网系”位置上,立足以小型机动车载装备和便携装备为主,以“沾染区外”的组织建立的指挥信息传输网络为依托,灵活地组织运用。通常“沾染区内”应由指挥车装载的短波电台、超短波电台、光学侦察设备、超短波视频传输设备、“北斗”导航定位系统用户机和便携式手持机、代码指挥终端、GPS设备等组成,并视情与“沾染区内”可利用的既设信息资源相结合,组织建立“沾染区内”的系统“末端网系”。

一是运用PDA代码指挥终端,结合GPS卫星定位系统,依托CDMA移动通信系统建立处置行动代码指挥网,为收集事发现场侦察信息,采集有关重要数据提供保障;为防化分队指挥员对下实施精确指挥与控制提供保障;为处置行动指挥部收集侦察情报、进行信息处理和利用计算机辅助决策提供数据与依据。“沾染区内”侦测组可通过代码指挥网,将查明的放射性污染积分浓度或毒剂种类与积分浓度,以及区内人员的中毒症状和有关情况,迅速传递给“沾染区外”处置行动指挥部或有关部门,以便于指挥机构及时、正确地做出处置决策和提示下风人员采取相应的防护措施,并为洗消分队提供行动所需要的放射性物质或化学物质的污染范围、空气中的积分浓度、持久性毒剂种类以及导航定位等各种侦察信息和数据,以便洗消分队迅速地展开行动;监测组可通过代码指挥网,将监测到的有毒空气的扩散及浓度变化情况、放射性物质辐射剂量变化及污染扩散情况、附近水域的受染情况以及洗消效果跟踪检测情况等及时上报,以便上级准确掌握处置行动的进展情况和可能发展变化的趋势,为指挥者提供重要的决策依据和数据。

二是“沾染区内”各专业分队可运用“北斗卫星定位系统”用户机,采集有关目标定位、行动导航和各种实体信息,将查明的沾染区范围、危害源

头、确定的受染边界、标志的受染区域等定位信息和实体信息及时向上报,以便指挥员确定行动部署和实施指挥控制。同时,为处置行动指挥员随时掌握防化分队行动路线、进展速度等提供准确的信息;为处置行动指挥部借助数字地图、定位信息测算出核化污染大致面积,勾勒出核化污染范围,提供相关信息及辅助决策依据;为处置行动指挥部通过短报文即时通信的方式,收集有关情况、调度与控制各专业分队行动提供辅助信息传递手段。

三是运用光学侦察设备、超短波视频传输设备,按指挥员的指示及要求,为“污染区外”处置行动指挥部提供重要地段、重要目标和污染受害者的当时实况,并根据需要将现场实况经“污染区外”组织建立的综合信息传输网络传送至高层指挥机构。

四是根据行动规模和污染区域的大小,视情运用短波无线台,建立“污染区内”指挥员对上的指挥联络,并经“污染区外”指挥信息系统中的异频交换设备加入“污染区外”组织建立的综合信息传输网,可在网内传递语音、电报、传真、数据等业务。重点保障处置行动指挥员与“污染区内”防化分队指挥员的指挥联络;保障处置行动指挥部与“污染区内”防化分队的信息传递与交换等。同时,为高层指挥者实施越级指挥提供保障。

运用超短波车载台、手持机,建立“污染区内”的无线电对讲机指挥协同网,并经“污染区外”的超短波基础台,加入超短波指挥协同网。重点保障“污染区内”防化分队指挥员对各专业分队(组)的指挥控制;保障处置行动指挥员对“污染区内”防化分队指挥员和各分队(组)的指挥与调度;保障“污染区内”各专业分队(组)与地方监测、洗消、医疗、消防、工程等力量的协同联络。

五是运用野战被复线、电话机、网线、笔记本电脑等,利用“污染区内”的军、民既设设施,组织建立起多路迂回、稳定可靠的信息传输网络,以利于“污染区内”指挥员能够通过此网加入处置核化事件行动时组织建立的综合信息传输网;以利于处置行动指挥部通过指挥控制分系统高效地实施指挥控制等。

## 2.2 “污染区外”的组织

处置核化事件时,我指挥信息系统的核心部分主要是开设在“污染区外”安全地带,不但可以展

开大型系统装备,建立高效的情报收集和指挥控制网,而且还可以充分利用就近的既设军民信息资源,建立较为完善的综合信息传输网络。同时,“污染区外”我网系组织建立的越完备,越有利于为“污染区内”提供信息支援与网络支撑,越有利于顺利地完全处置任务。

一是运用卫星机动通信站,按处置核化事件行动的总体部署和指挥信息系统组织运用方案,以各卫星机动通信站为网系节点,采用分布式组网方式,快速组织建立远程、大容量、多业务的信息传输网,并视情通过野战光缆、微波接力或既设通信设施接入国防信息传输骨干网,构建满足处置核化事件需要的综合信息传输网络,为组织建立较为完备的指挥信息系统提供有利条件。

二是运用指挥信息系统的代码指挥功能,通过CDMA移动通信系统或超短波通信链路组织建立代码指挥网,为处置行动指挥部接收“污染区内”各专业分队发回的情况报告和指挥控制各专业分队行动提供保障。

三是运用野战机动指挥方舱装配的计算机服务器、路由器、网络交换设备、无线网桥、EDSL设备等,采用辐射状星形组网的形式,快速组织建立处置行动指挥部局域网,为指挥控制分系统组网运行提供前提条件。通常在处置核化事件行动中各指挥要素将集中开设,以便于指挥员迅速组织研究处置方案。因此,处置行动指挥部局域网的建立,以网络交换机、网线或无线网桥设备 etc 为主,快速组网,并依托卫星机动通信站建立综合信息传输网,为指挥控制分系统组网运行提供支撑。在此基础上,使用系统的各种指挥作业应用程序,构建起处置行动中的指挥控制平台。其中,指挥部可根据“污染区内”发回的侦测、监测信息和数据,对有关情况进行计算和照射剂量进行测算,为正确使用力量和确定防护措施提供依据;可运用指挥信息系统的查询功能,查询有关核化物的属性、危害及消解与防护措施,查询事发地的地理、水文和气象信息,并以人机交互的方式,调用系统数据库,优化处置行动方案或进行预案优选,辅助指挥员决策;可运用数字地图处理子系统,进行标图作业,并通过视频显示系统输出有关情况;可运用系统的文图处理功能,接收上级命令、指示和“污染区内”的情况报告,快速拟制或修订指挥文电与报表,迅速上传下达。

四是运用车载短波无线电台、便携式超短波无线电台,组织建立部队对上、对友邻和对下的无线电台指挥信息传输网及指挥联络专向,在网(专)内可传递代码指令、数码电报、数据传真、计算机数据和电话业务。同时,运用异频交换设备、转换接口设备、网络程控交换设备等与综合信息传输网络相联接,拓展指挥信息传输网系边际。

运用超短波基地台、车载台和手持机,组织建立无线电对讲机指挥网,并通过异型电台转接设备,加入综合信息传输网络。通常在已明确的受染边界外适当地点,开设超短波基础台,力求电磁信号能够覆盖“污染区内”防化分队的主要行动区域,以便建立起“区外”与“区内”互通的超短波指挥网络。

五是运用超短波视频接收机,与“污染区内”的超短波视频发信机构成超短波视频传递链,接收“污染区内”侦察车发送回的视频信号,并经由网络交换设备、音视频控制矩阵、视频显示系统等,为处置行动指挥部提供现场实况。同时,根据上级要求或首长指示,将现场实况影像通过综合信息传输网络,远程提供给高层指挥机构。

六是运用信道加密和终端加密设备,对信息传输网系实施加密保护;对我指挥信息系统与其他网系互联互通实施加密保护,以确保我重要信息传递的安全保密,确保高级指挥员实施超常指挥时的安全保密,确保高密级指挥文电传递的安全保密等。

当我在边境地区遂行处置核化事件任务时,应根据事件的性质和上级要求,预有准备,充分做好指挥信息系统的安全防护工作,以防备外部势力为扰乱我处置行动,对我指挥信息系统实施干扰与破坏。

### 3 处置核化事件中指挥信息系统组织运用应重点把握的问题

处置核化事件行动中,应当针对其事件特点和对指挥信息系统组织运用所产生的主要影响,在组织建立指挥信息系统及其网系时,应当全面了解事件的发展变化情况及其性质,区分“污染区外”与“污染区内”的不同,依地形地势、当时天气和风向等因素,周密地组织建立指挥信息系统。组织实施中,系统各要素在开设与撤收时应注意把握以下几点:

一是“污染区内”是事发的重灾区,周围环境到处都存在着放射性污染物或化学污染物,对我人员和指挥、侦察、通信装备构成严重威胁。现实环境的严酷性,致使我高度集成的大型系统装备在非战争状态下,不可进入核化污染的烟羽区内,以免事后因难以洗消而导致装备废置,造成更大损失。在“污染区内”,各种装备和器材应尽量不落地,降低污染程度,以利于事后洗消和维护。撤收时,所有车辆和装备器材必须严格消洗,并单独存放。

二是处置核化事件时,我指挥信息系统的大型装备可在“污染区外”安全地带,利用就近的既设信息资源展开,力求建立较为完善的综合信息传输网络,以利于为“污染区内”的系统“末端网系”,提供多途径的入网节点和网络支撑。故此,“污染区外”我指挥信息系统组织建立的越完备,越有利于为“污染区内”提供信息支援与支撑,越有利于顺利地完全处置任务。

三是在烟羽区架设必要的线路时,通常不埋设,必须埋设时人员应站在上(侧)风方向,先清除地面污染物,而后埋设;线路高架时,要利用悬线杆高挑架设。撤收时受染线料必须与其他物品分开存放。

#### 参考文献

- [1] 《中国人民解放军司令部工作条例》. 北京: 军事科学出版社, 2006 年
- [2] 沈树章、王应泉.《突发事件通信》. 北京: 解放军出版社, 1995 年
- [3] 沈树章、王祖平.《通信指挥手册》. 北京: 解放军出版社, 2005 年
- [4] 叶西荪、南 庚.《军事通信网分析与系统集成》. 北京: 国防工业出版社, 2005 年

#### 作者联系方式

通信地址: 通信指挥学院战役通信教研室

邮政编码: 430010

联系电话: 027-85968350 13397161559

# 区域联合电磁频谱监测管理系统研究

吴冠 张超 杨俊明

**摘 要:** 区域联合电磁频谱监测管理系统是在复杂电磁环境下, 保证战术级联合部队合理使用其电磁装备的有效手段。本文首先分析了区域联合电磁频谱监测管理系统的内涵、功能、组成和工作流程, 最后对此系统的关键技术及其面临的问题进行了讨论。

**关键词:** 区域; 联合频谱; 监测与管理

战场电磁频谱监测管理系统是监测电场电磁环境和管理本方电磁设备的综合化军事信息系统, 它是现代战场管理系统的重要组成部分。

从作战层次来看, 战场电磁频谱监测管理系统由国家、战区、战术三个层次组成, 其中区域电磁频谱监测管理系统(以下简称系统)应用于战术级部队的作战区域, 是国家和战区电磁频谱监管的基础和数据来源, 因而具有特别重要的地位。

## 1 战术级联合部队的特点

战术级联合部队(以下简称联合部队)的合成性主要体现在武器装备和人员编组上。联合部队普遍装备有多种无线电台、雷达、电子对抗器材和导航仪等电磁装备。这些电磁装备很容易互相干扰, 使得彼此都无法正常工作。另外, 联合部队还要面临来自民方、敌方和友方部队的各种无意的和有意的干扰。可见联合部队具有电磁装备多、容易互扰和干扰源多的特点。

## 2 区域联合频谱监测管理系统的内涵

区域联合频谱监测管理系统是用于完成战术级联合部队作战区域内电磁环境的实时监测和频谱资源的统一管理的综合信息系统。

区域联合频谱监测管理的对象是联合部队作战区域内的电磁设备。监管对象的分类相当多样, 从敌我性质上讲有我方、敌方和民方之分, 从平台位置上讲有空中(包括太空)、地面和海上(包括水下)之分, 从用途上讲有通信、探测、干扰、导航之分等。常见的电磁设备有无线电台、卫星导航

仪、雷达、电子对抗器材等等。

区域联合频谱监测管理的内容是作战区域内的无线电频谱。国际电信联盟将无线电频谱定义为 3kHz 到 3000GHz。但目前由于技术条件的限制, 仅能利用 300GHz 以下的频率, 不到划分总量的十分之一; 而现代通信信号占用的频率范围只有 2MHz~14GHz; 在指定的作战区域内, 通信信号占用的频率往往更窄, 大多数为 2MHz~500MHz, 雷达和雷达干扰机的工作频率范围可达 0.1GHz~18GHz, 但在多数地域, 它们的工作频率主要集中在 1GHz~18GHz。故区域联合电磁频谱监测管理系统应对 300kHz~18GHz 之间的频段监管, 而在实际作战中, 某一联合部队作战区域内电磁装备所占用的频谱可能只有很窄的几个频段, 因此只需对部分频段进行监测管理即可。本文将系统需监测管理的所有频段统称为监管频段。

## 3 区域联合频谱监测管理系统的功能

区域联合频谱监测管理系统具有如下功能。

### (1) 区域电磁背景显示

区域内所有电磁装备的使用均受到该区域电磁环境的影响, 系统需具备在电子地图上以可视化的图形方式实时显示作战区域内电磁环境背景的能力。频谱具有频率维、功率维、时间维、空间维和信号维五种认知维度, 因此可以用这五个维度来显示区域内的电磁背景环境。战场电磁环境具有动态性的特点, 因此要求电磁背景显示具有实时性(或近实时性)和持续性。

### (2) 电磁设备监测与显示

系统可在电子地图上以图形方式近实时地显示合成旅作战区域内敌我电磁设备的分布情况, 并显

示电磁设备的所能感知的全部属性,如敌我性质、类别、型号、使用频率的五维特征等。

### (3) 区域电磁兼容与干扰分析

系统可根据本方电磁设备的分布和性能参数,分析本作战区域内的电磁兼容性,采取措施以避免设备间的相互干扰;同时,依据对作战区域内敌方电磁设备的监测结果,系统可分析其对我方设备的干扰情况。区域内的干扰包括噪声干扰、同信道干扰、邻信道干扰、互调干扰和远近效应。

### (4) 区域频段质量分析

系统可结合电子地图,通过地形、地物、天线角度、电离层状况、气象状况、电磁设备性能参数等数据,对监管频段进行质量分析和预测,以获得最优的频谱使用质量。

### (5) 区域频率分配

根据区域链路质量分析的结果,结合本方电磁设备性能参数、数量、分布和用频需求,系统可为本方各电磁设备统一分配工作频率,以避免电磁设备间的相互干扰,并降低发射功率,达到最优化利用频谱和降低暴露本方目标的目的。

### (6) 电磁及地理信息数据存储

系统应利用数据库保存敌我电磁设备的性能参数、作战区域地理信息、频谱资源和历史频率管理方案和提前制定的频率使用预案。

### (7) 作战信息交换

区域频谱监管系统本身就是一个通信系统,可与同级系统交换信息,可向上级部门上报区域频谱信息,可向火力打击部门发送作战情报。

## 4 区域频谱监管系统的组成

区域联合频谱监测管理系统由三个分系统组成,分别是探测与通信分系统、频谱监测管理工作站分系统和装载平台分系统。

从硬件组成来看,探测与通信分系统分为频谱监测器、探测发射机组、探测接收机组三个部分(由于软件无线电技术的发展和运用,目前普遍将探测与通信设备融为一体)。

频谱监测器用来接收监管频谱波段的电磁波,测定区域内监管频谱波段的场强和频谱占用情况,以显示区域内的电磁背景。

探测发射机组和探测接收机组本质上分别是基于软件无线电的多频段、多波束发射天线和接收天

线,其频谱范围必须包括监管频谱。目前的趋势是在通信系统中直接采用实时信道估值技术,将探测与通信融为一体。

探测发射机组的作用是发射探测信号和通信信号。在进行信道探测时,发射天线在需要探测的频率范围内发射探测信号,探测信号的形式是线性调频连续波,其频率随着时间作线性变化。在接收端,由一部与探测发射机同步工作的探测接收机接收和处理探测信号,并将结果输入到频谱监管工作站。接收端可与探测发射机不处于同一装载平台。在进行通信时,探测发射机组的作用是发射无线电信号,目标天线接收到通信信号后,可以将通信质量反馈回系统以评估信道质量。以软件无线电为基础的探测发射机组能以不同的波形、不同的调制方式与不同波段的电台进行通信。

探测接收机组的主要作用是接收无线电信号并依此进行信道探测。信道探测分为有源和无源探测两种方式。接收机组接收来自发射机组的探测信号,依此评估信道质量,这就是有源探测。无源探测是指不需要专门发射探测信号,而只是检测信道的噪声和干扰水平,利用信道背景的特性来间接评估信道的质量。

频谱监测管理工作站分系统包括频谱监测管理软件和计算机支撑环境,其中前者是此分系统的核心部分,计算机环境包括计算机硬件、网络、操作系统、地理信息系统和支持数据库等等。

为了便于实现、维护和复用,将频谱监测管理软件划分成三个层次,分别是应用层、数据库层和数据获取层,如图1所示:

频谱监测软件应用层包括上面所定义的7项功能,数据库层和数据获取层的组成如图1所示。数据库层中,地理信息数据库包含联合部队作战区域的电子地图和各类军事图标;电磁设备数据库包含联合部队、民方和敌方的已知电磁设备的性能参数;频谱资源数据库包含联合部队作战区域可使用的电磁频谱资源和频谱资源使用情况;使用信息数据库存储以往频谱使用方案(含质量评估)、提前制定的频谱使用预案;模型数据库存储电磁兼容模型、干扰模型、频段探测模型、频谱分配模型等,它是频谱监测软件的工作规则。数据获取层负责接收电磁背景监测、无线电定位与识别、无线电频段探测三种信号以作为频谱监管的依据。

装载平台分系统是区域频谱监管设备的载体,

可以是地面固定站、机动通信车、飞机、水面舰艇、停空气球等。

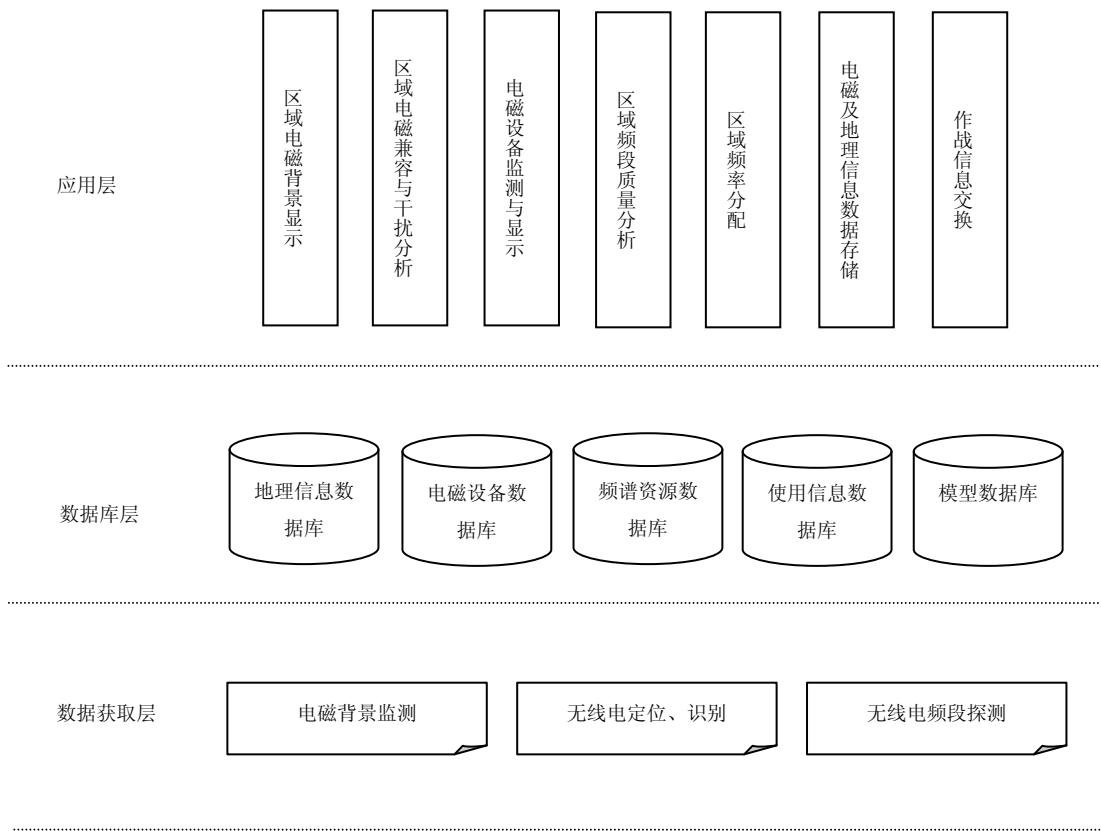


图 1 软件层次结构

5 区域联合电磁频谱监测管理系统的  
关键技术及其面临的问题

区域联合频谱监测管理系统的核心技术是探测与通信系统中的软件无线电（SDR）、无线电测向与定位、频段质量探测，其中软件无线电是核心技术。

软件无线电的特点是系统的主要功能主要由软件实现，是在通用的硬件平台上通过软件的不同算法，实时配置自己的信号波形、调制方式，提供不同的无线探测和通信能力。软件无线电由六个关键部件组成：多频段、多波束天线与宽带射频，高速数字信号处理部分，宽带 A/D 部分，高性能的互联结构，以及软件协议和标准。目前天线与射频部分一般采用组合式多波段天线，如美军的 Speakeasy 系统的天线由 3 副不同频段（3MHz～30MHz、30MHz～500MHz、500MHz～

2000MHz）的天线组成。

目前软件无线电发展的瓶颈在高速数字信号处理部分。一般认为要进行较好的滤波处理，需要每采样点 100 次操作，对于一个系统带宽为 10MHz 的系统，采样率需大于 25MHz，这就需要 2500MIPS 的运算能力，目前的数字信号处理芯片还无法完成这一任务。为了解决这一问题，可采取的方法有：一是研制各种新的数据处理芯片，即“数字信号处理器（DSP）和现场可编程门阵列（FPGA）、专用集成电路（ASIC）并举，通用型 DSP 和专用型 DSP 并举”；二是采用优化的采样算法。

软件无线电发展的另一个难点在于如何实现高性能的互联结构，该部分的功能是实现系统中各功能单元互联，组成一个开放、可扩展的硬件平台，同时具有较高的数据吞吐率。

在联合部队作战区域内，为了减小被敌发现的概率，无线电定位和识别、频道质量分析必须向无

源探测方向发展。无源探测方式不仅无需探测发射设备，自成一体，独立性强，而且具有很好的隐蔽性，也不会对因探测信号的发射而对其他用户造成

干扰，但是其精度和可靠性仍有待进一步的研究和改善。

### 参考文献

- [1] 王汝群等，战场电磁环境，北京：解放军出版社，2006
- [2] 张跟全、马飞、李大艳，国家频谱管理系统的分析与设计，2006，无线电工程，第 36 卷第 10 期
- [3] 贺志超、王荣，机械化部队频谱资源管理与分配系统的设计，装甲兵工程学院学报，2000 年第 14 卷第 3 期
- [4] 杨君，刘云，基于 MapX 的通信资源管理系统的设计与实现，2003，中国数据通信，第 5 期

### 作者联系方式

通信地址：湖北省第二炮兵指挥学院研究生管理大队三队

邮政编码：430012

联系电话：027—51252334



# 基地防御战斗中的电子对抗

巫银花 陆勤夫 陈永芳

**摘 要:** 以近年的几场高技术局部战争为背景,对电子战在海军基地防御战斗中的使用和战术运用情况进行了研究。对在海军基地防御中电子战现状及采取的对策进行了分析,并对未来基地防御战斗的电子对抗提出设想和展望。

**关键词:** 海军基地; 防御战斗; 电子对抗

## 1 引言

伊拉克战争中。美英联军之所以自始至终都掌握战争的主动权,其中一个最根本的原因就是美英联军掌握了战场的制电磁权(信息权),美英联军大量使用了最先进的电子战装备<sup>[1]</sup>,包括星载、舰载、机载、陆载以及投放式电子战装备,对伊拉克的电子设备进行了有效的干扰,为取得战争胜利起到了决定性作用。考虑到未来战争的信息化特点,如何在海军基地防御中利用好现有的电子战装备,以最佳的组织手段和战术、技术措施来抗击敌人的电子进攻,在海军基地防御战斗中具有重要的地位和作用。同时为了应对信息化条件下的战争我军基地必须实现电子对抗的“网电一体”化。

## 2 海军基地防御中电子对抗面临的问题

从近年来的几场高技术局部战争,特别是在这次美英联军对伊拉克的战争中,我们可以明显地看到进攻方和防御方之间武器装备上的差距。这也在一定程度上代表了未来海军基地防御面临的情况。从伊拉克的防御中,我们可以看到目前海军基地防御中面临许多共同的问题。

一是指挥信息系统落后。首先目前防御方的指挥系统情报的获取能力非常有限。一般没有太空和空中的侦察平台,能够侦察的频段又比较窄,特别是在超低频和超高频段的侦察设备几乎没有,对像美国这样的军事强国的新体制的电子系统也缺少侦察手段,缺少先进的情报处理自动化系统,得到的信息不能及时处理。在受到敌方电子干扰的情况

下,难以保持信息的有效传递;其次是辅助决策能力弱,在电子对抗的指挥中,仍以人工决策为主;第三是指挥系统反馈信息能力弱,无法实现有效的电子对抗控制;第四是电子对抗作战没有完全进入联合作战信息系统。

二是防御的目标众多。因为是基地防御,包括对港内设施、港内船舶、陆上的主要军事目标、军事设施以及一些民用设施等的防御。这就要求在防御战斗中防御方需要防御的目标很多,电子对抗的任务繁重。

三是没有战斗的主动权。因为是防御战斗,所以战斗的主动权是由进攻之敌掌握,进攻方的快速发起战斗可对防御方达成突然强烈的电子进攻。

## 3 海军基地防御中电子对抗对策分析

### 3.1 统一指挥,密切协同

要搞好基地防御战斗中的电子防御,首先要统一建立信息作战指挥机构,统管战斗方向上各战术兵团的电子防御工作。一是建立上下一体的信息指挥机构。在指挥体制上,实行纵横式网状指挥,实现情报共享,统一协调各信息作战要素的作战行动;二是战斗最高一级信息作战指挥中心应统一拟制基地电子防御计划,重点加强电子对抗分队之间、电子对抗分队内部、电子对抗与非电子对抗分队之间的协同,合力抗敌;加强电子对抗分队与技术侦察分队和雷达侦察分队之间的协同,提高情报侦测能力;加强电子对抗分队与技术侦察分队、火力群的协同,提高整体作战效能。

### 3.2 合理部署，整体防御

首先是合理部署电子防御体系。在基地防御中，电子干扰系统的部署十分重要。它要求必须能及时发现与引导目标担负侦察引导任务的兵力兵器应配置在有利地形，以便尽早远距离发现敌目标，及时对干扰兵力实施引导；在全面部署的基础上，主要干扰兵力应当部署在敌来袭目标主要方向上，并且能对重要目标较好地实施电子防御；在组织管理上，电子干扰配系应当由基地统一组织建立，以便于指挥协同。干扰兵力的战斗部署，应以发挥最佳干扰效果为目的，同时要避免己方各种电子设备之间的相互干扰。考虑到进攻方反辐射兵器的袭击，防御方的电子装备在部署时必须充分考虑到机动性和隐蔽性。

其次是正确配置电子干扰兵力。一是当已知进攻方航空兵、导弹来袭方向时，对空雷达干扰兵力应配置在掩护目标与来袭兵力之间，对空雷达干扰兵力可采用线状配置，也可采用扇形配置；二是当不清楚其航空兵、导弹来袭方向或敌航空兵可能实施多向空袭时，对空雷达干扰兵力一般采用环形配置；三是掩护己方在政治、军事上具有重要意义的目标时，应采用梯次配置，以环形配置或扇形配置为基础，在主要方向采取多层次的扇形配置样式，以形成大纵深的干扰空域；四是地对空雷达干扰站应配置在制高点或海岸岛屿的突出部位，以取得最小的遮蔽角，获得尽量大的侦察和干扰空域；五是无线电通信干扰兵力应当配置在安全隐蔽的高地或山头。

### 3.3 隐真示假，真假互换

隐真示假，真假互换，是指运用伪装、佯动等电子欺骗手段，制造假象，隐蔽企图，并通过真假通信联络任务的相互转换，欺骗和迷惑敌人，以求形成对我有利的通信态势。

首先，隐真、示假要有机结合，使敌方难辨真伪。“隐真”，即通过电子伪装（使用伪装网、角反射器或使用吸波材料和低反射涂层），可以改变在敌侦察卫星、侦察机、导弹末制导雷达等回波中的海军基地的地形、地貌，使之错误地引导或跟踪。另外，可以通过人为制造一些假的目标，如假机场、假飞机、假发射阵地等等，吸引敌人的火力，使其火力资源的效费比大大降低。例如，在海湾战

争中，伊拉克军队广泛使用充气坦克、充气飞机、充气导弹发射架以及假防空导弹阵地等假目标，结果使多国部队多次攻击失效，白白浪费弹药；其次，真假互换，真真假假。一是工作网与佯动网互换，工作网与佯动网都担负着双重任务，当遭敌干扰无法工作时，佯动网适时转换为工作网，接替工作网工作。当佯动网遭到敌干扰无法工作时，工作网可视情接替佯动网工作；二是工作网与干扰台互换，利用干扰台发信，在连续播放干扰信号的间隙，突然转换发送我方指挥信息。例如，干扰台在某频率上施放干扰信号，造成对方侦听后认为该频率为干扰频率，放弃干扰。当有报（话）时，即可用此网工作，工作完后又施放干扰，使敌人不易判断真假。工作网在遭敌干扰时继续工作，以吸引敌人，掩护干扰台工作，当敌人不干扰我工作网时，工作网照常工作。

### 3.4 “软、硬”兼施反击防御

海湾战争中，美军将电子侦察、电子干扰与电子摧毁结为一体，形成现代战争电子战的新趋势。例如，EA-6B 电子战飞机在侦察干扰的同时，还可以直接发射导弹直接攻击雷达系统。对此，在未来的高技术战争中，不仅要注意电子软毁伤，还可以发射反辐射导弹直接攻击雷达系统。对此在未来的高技术战争中，不仅要注意电子“软”毁伤，而且要注意电子“硬”摧毁的后果。

海军基地防御中电子战进攻力量的重点是干扰和摧毁主要作战方向进攻方的重要电子系统和设备，掩护己方重要目标和其他友邻部队对进攻方采取反击性军事行动。

运用电子战“软、硬”杀伤手段，对敌电子战部队的指挥通信系统实施干扰压制、对敌干扰辐射源实施火力摧毁等进攻行动<sup>[2]</sup>，以掩护我通信系统正常工作的以攻为防的通信防御方法。有效的防御应是积极的防御，力求从被动中争取主动。为此，必须将通信进攻寓于通信防御之中，积极采取通信干扰、火力打击等手段，干扰和摧毁影响较大的敌电子战系统。特别是在通信防御技术手段不足的情况下，或者在我主要通信系统遭敌强烈干扰而无法摆脱时，更应突出攻势防御在通信防御中的运用。运用反击防御方法，一要优选打击目标，应将威胁最大的敌通信干扰源及侦察设施作为首选目标；二要合理选用打击手段，根据目标的性能选择相应的

通信干扰手段。通信干扰的频段,应与我方电子设备的工作频段相区分。如果干扰手段不足以达到目的,则应果断采用火力打击手段。三要正确选择打击时机,应与部队作战行动时机相协调,通常选择在作战的主要阶段和关键时节特别是遭敌电子战压制无法摆脱时。

### 3.5 多法并举,全民动员

基地防御战斗中,仅靠我有限的信息作战力量是不够的,还需全民动员,利用各种力量,通过各种渠道,对敌实施全面的电子防御。一是加强同友邻国家、地方信息力量的情报交流,积极拓展各种信息侦察渠道,对敌进行信息侦察,及时、准确地掌握敌进攻动向,为实施有效的电子防御做好准备。二是通过通信工具、刊物、广播、电视和拟定假作战文书等手段,散布假信息,误导敌进攻准备。海湾战争中,美军用飞机和火炮将传单投放到伊军阵地共投放了 2900 万份,用“海湾之声”电台进行广播,从 1 月 19 日开始,每天播音 18 小时,连续进行 40 天,在地面部队旅以上单位建立“高音喇叭小组“,通过阵地喊话,鼓励伊军士兵放下武器投降。以上措施取得了良好的心战效果。三是全民动员,广泛建立有线电通信和自动化指挥网络,确保在基地防御战斗中,能进行情报快速传递和使用指挥自动化系统指挥作战。

## 4 对未来海军基地防御战斗中电子对抗的设想和展望

海湾战争中,以美国为首的多国部队,平均每天出动 2600 架次飞机对伊拉克进行狂轰滥炸,平均每分钟就有两架次飞机起落。然而多国部队却能把这一切组织的有条不紊,靠的是构成网络的计算机指挥控制系统。由此可见,信息化条件下的战争对未来海军基地电子对抗提出了新的要求。

### 4.1 构建信息化的武器系统

信息化武器系统<sup>[3]</sup>由三部分组成:信息化弹药、信息化平台和 C<sup>4</sup>I 系统。信息化弹药实质上是指是一种能够获取和利用被攻击目标所提供的位置信息修正自己的弹道以准确命中的弹药。信息化作战平台是指有人驾驶的作战平台,如飞机、舰艇、

潜艇等都将安装大量的电子信息设备,有多种信息设备与上级和友邻部队互通作战信息,成为 C<sup>4</sup>I 系统的一个节点。信息化作战平台除了利用己方和对方的信息能力外,还有防御敌方利用自己的信息的能力,这就是具有侦察、干扰、欺骗等功能的电子战设备。整个信息化武器系统的神经中枢是 C<sup>4</sup>I 系统,其作战行动将是以 C<sup>4</sup>I 系统为代表的自动化作战系统控制下进行的,并以 C<sup>4</sup>I 系统对抗为核心内容展开信息获取权、控制权与使用权的全面争夺战。因此,现代战争中信息战攻防尤为重要。应综合使用基地编队电子对抗力量及其他电子支援兵力,大力提高现有装备的整体效能。利用信息技术和横向一体化技术,对基地电子战系统进行信息化改装或改进,将其连接成互联互通的一体化系统,可加速电子战系统及各作战单元之间的信息流动,从而大幅度地提高其整体功能,必须充分重视空中、水面、水下及岸上电子支援兵力的建设。

### 4.2 实现电子对抗的“网电一体”化<sup>[4]</sup>

针对信息网络在现代海战中不可或缺的重要作用,应在传统综合电子战思想基础上树立“网电一体”对抗思想。现代海战模式已逐渐从“平台中心战”转向“网络中心战”,强大的信息网络可将战场上各种探测装置、指挥中心及武器合成为一个统一高效的大系统,从而极大地提高其整体作战能力。信息网络已经成为现代海战中必不可少的“神经系统”。海湾战争及伊拉克战争都是首先从网络打击开始的,由于伊拉克缺少相应的网络打击能力,从而使战争出现严重失衡情况。美军甚至认为:网络将成为未来提高战斗力的唯一重要因素。海军基地防御战斗同样离不开信息网络的支持,所以基地防御战斗电子对抗不仅要注重“制电”,更要注重“破网”。只有做到“网电一体”,才能真正具备系统对抗的能力。可以预见,“网电一体”将是未来基地防御战斗电子对抗的主要趋势。为此,我们在基地防御战斗“软抗击”系统的建设过程中,必须重视“网电一体战”技术和装备的发展,同时具备电子战和网络战的综合对抗能力,力求以“网电一体化进攻”的积极姿态破坏敌方各级各类 C<sup>4</sup>I 系统的关键节点,瓦解和瘫痪敌方的侦察预警、作战指挥及火力控制等系统。即集中精锐,打敌要害。总体上讲,海军信息作战能力与交战对手相比优势不明显,要确保完成信息作战任务,就要统一计划

和使用精锐的武器装备和作战力量,超常编组、超常用兵,以我精锐,选择敌作战依赖较大,并可对其军事信息系统产生重大影响的薄弱环节实施攻击,确保在关键时节和重要时机,对敌能形成重锤猛敲、打狠打痛之势。同时,要想在将来赢得信息

时代战争的主动权,就必须保护好自己的信息与网络系统,只有保证己方的信息系统畅通无阻,才有能力和机会进攻和破坏敌方的信息系统,取得信息优势,从而打赢信息战。

### 参考文献

- [1] 尹烁莹.现代战争中电子战装备及作战特点[J].火力与指挥控制,2001,26(4):12-14.
- [2] 季广智.防电子干扰基本方法浅探[J].指挥学报.2001,(5):1-8.
- [3] 陆勤夫,何常青.海上与岛屿作战战例评析[M].北京:海军出版社.2002.
- [4] 庄振明.光电子对抗的回顾与展望[J].飞航导弹.2000(2):55-59.

### 作者联系方式

通信地址:南京海军指挥学院海战实验室

邮政编码:210016

联系电话:025-80840086

# 野战通信资源自动配置系统的开发

谢晓霞 史勇 牛康伟

**摘 要:** 该文针对人工配制野战通信资源时存在的问题, 根据专家系统的原理, 运用模糊数学、军事运筹等理论, 结合部队实际设计了野战通信资源自动配置系统的结构框架、功能。文中具体介绍了数据库、模型库、知识库领域内知识表示方法和智能推理策略等内容。本系统主要应用 Visual C++6.0、Visual Prolog6.1 和数据库技术设计实现, 其中 Visual C++6.0 主要用来开发图形用户界面和进行后台处理, Visual Prolog6.1 主要用来设计推理机, 而数据库技术则用来存储在推理中要用到的规则。

**关键词:** 专家系统; 野战通信; Visual C++; Visual Prolog

## 1 引言

根据新时期军事战略方针和加强指挥自动化建设的精神, 立足现有通信装备, 着眼未来高技术的发展, 深入研究现代化战争中战略作战国防通信网在各种作战样式中的组织运用, 以适应未来战略作战的需要, 是摆在我军面前的一项急待解决、事关全局的重要任务。但随着通信技术的发展, 通信保障将展开、配置在几千平方公里的作战地域内, 其涉及的设备众多、技术密集、机动性强、连接关系和层次复杂, 在这种情况下, 若要在较短的时间内, 针对作战任务, 对通信兵作战行动中的兵力、装备、器材、物质、时间、空间和自然资源等进行合理的计划、分配, 并能制定出多种通信保障方案进行比较和优选, 仅靠传统的人工配置通信资源的方式就很可能造成顾此失彼, 通信资源应用不当, 或不能进行多方案优选而延长了组织指挥时间。

目前, 我军尚无一个功能齐全、性能可靠的可供通信首长、参谋、机关使用的功能齐全、性能可靠的通信资源配置系统。因此有必要借助计算机技术, 应用专家系统和军事运筹等现代化技术组建适合我军现状和未来发展的野战通信资源自动配置辅助决策系统, 使我军的通信保障能力日趋实现自动化。

## 2 系统设计与分析

### 2.1 系统的设计思路

该系统是基于专家系统的原理, 利用军事运

筹、模糊数学的知识, 结合通信组织的原则等, 通过计算机语言 Visual C++ 6.0、Visual Prolog 6.1 和 SQL Server 2000 实现的软件系统, 如图 1 所示。在系统的实现上, 我们采用 Visual C++ 6.0 语言设计人机界面和进行后台处理, 同时对综合数据库和知识数据库进行管理, 通过推理机的推理, 返回并解释所得方案。其中综合数据库、知识库采取 SQL Server 2000 语言编写。推理机采用 Visual Prolog 6.1 编程实现。

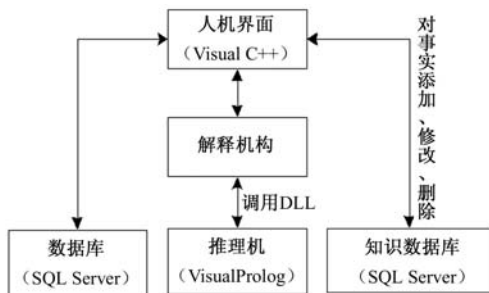


图1 系统设计思想

### 2.2 系统的体系结构

本系统依据专家系统的基本结构, 构建系统的体系结构如图 2 所示。各模块的功能简述如下:

- 人机接口: 用户提供直观、方便的交互手段。
- 知识库: 这是专家知识、经验和书本知识、常识的存储器。
- 综合数据库: 存储领域内的初始数据和推理过程中得到的各种中间信息。

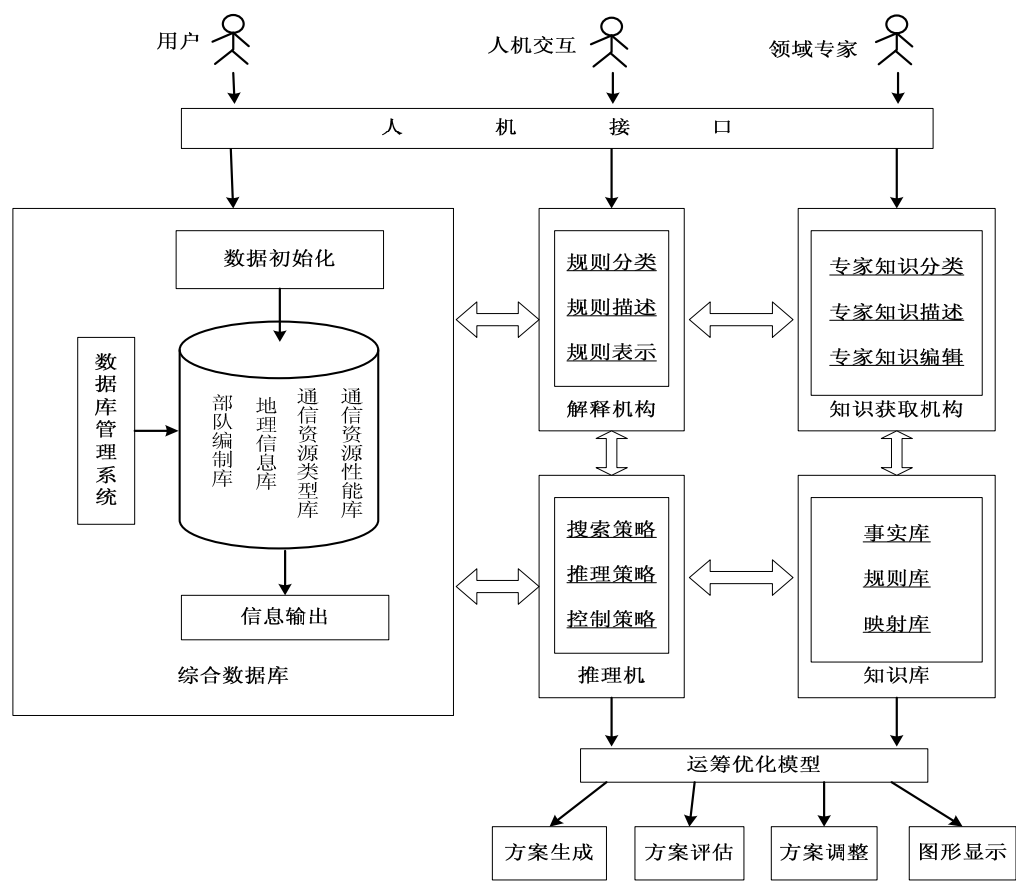


图2 系统体系结构

- 推理机：是一组程序，有它控制、协调整个系统，并根据输入的数据（即数据库中的信息），利用知识库中的知识，按照一定的推理规则和控制策略，对所求解的问题进行求解。

2.3 系统的功能设计

该系统的主要功能为：根据作战（演习）意图和作战（演习）需要，辅助通信指挥人员对通信资源进行有效调配，迅速形成通信保障方案，并对生成的多套方案进行评估和排序，给出最优方案。其具体功能如图 3 所示。

(1) 资源数据库管理

建立并管理各种数据库。如部队编制数据库、车辆、设备数据库、地理信息数据库等。数据库管理操作功能包括数据录入、查询、修改、删除等。

(2) 知识库的维护

建立并管理各种通信组织原则、作战手段、组

- 解释机构：向用户解释系统的行为，包括解释结论的正确性及系统输出其他候选解的原因。
- 知识获取机构：它为修改、扩充知识库的知识提供手段。

网原则等与通信资源配置相关的知识。知识库管理操作功能包括知识的录入、查询、修改、删除等。

(3) 通信资源配置方案的形成

根据我军通信指挥原则，以集团军或师战役想定为基础，针对不同的地形、气象、指挥方法、敌方情况、各种战场参数等，可短时间自动生成通信资源配置方案，并使之满足整个作战区域指挥通信的需要。

(4) 方案评估

根据基本业务指标和战术指标，对自动生成的通信保障方案或人工输入的通信保障方案进行评估，并进行比较优选，从而选出最佳通信保障方案。

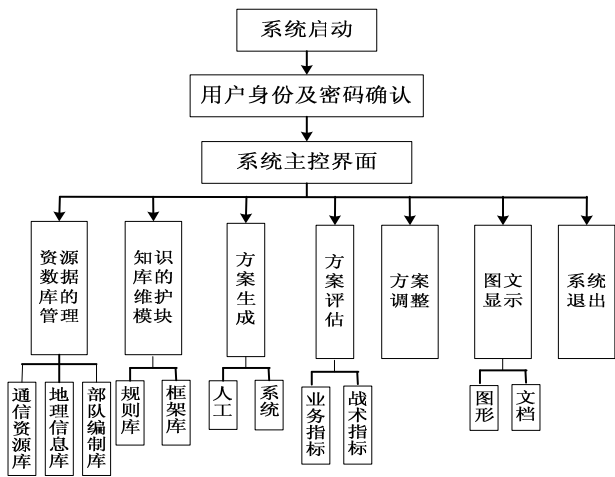


图 3 系统功能框图

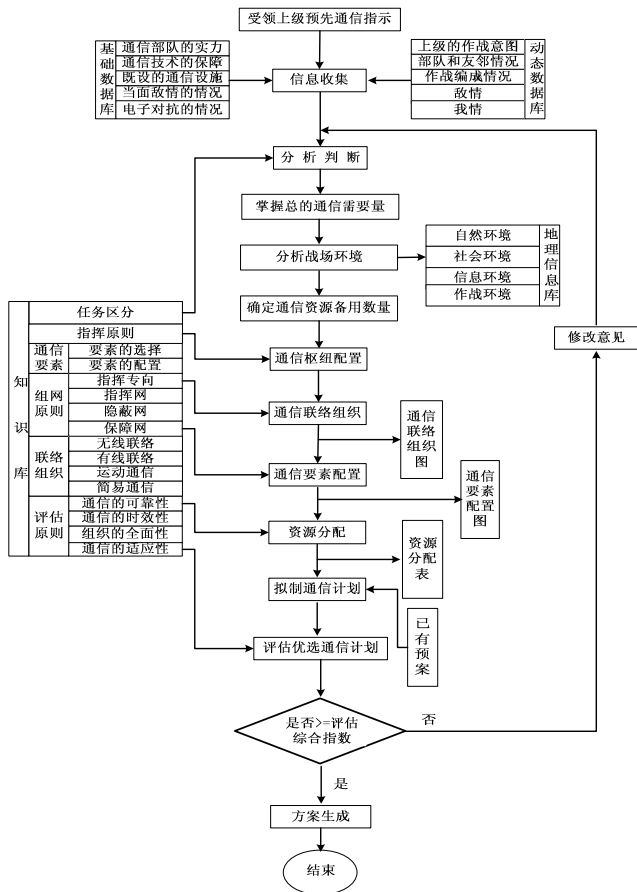


图 4 系统逻辑流程图

(5) 通信保障方案的调整

打印输出。

可根据评估指标，或人工设定的参数自动调整通信保障方案，使其通信保障方案指标达到最优。

- 以表格形式打印输出各种评估指标。

(6) 图文显示

2.4 系统的流程图

- 以二维/三维方式显示战区地形、通信资源配置图。
- 对形成的通信资源配置方案以表格的形式

基于现行人工配制通信资源的流程，我们设计了系统的逻辑流程，如图 4 所示。

3 系统的实现

3.1 综合数据库

综合数据库中存储的内容为系统运行时，所需的基本数据和推理时产生的中间数据。本数据库将分为静态数据库和动态数据库，静态库中存入预先输入的数据，如通信资源性能、部队编制等；而动态数据库存储实时数据，如演习时的想定数据等，具体内容如图 5 所示。本数据库统一采用 SQL Server 2000 进行编写和存储。

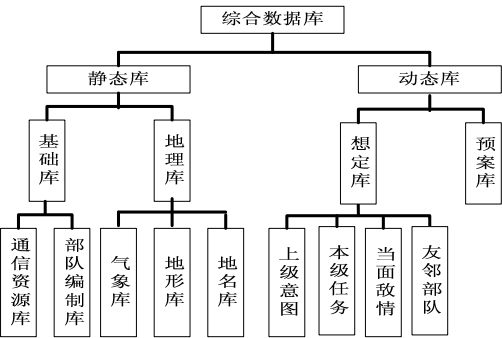


图 5 基础数据库内容

3.2 知识库

3.2.1 知识库中内容

知识库是数据库在知识领域方面的扩充，其实质仍为数据库。本系统中的知识库，采用 Visual Prolog 6.1 进行编写，其优点为 Visual Prolog 6.1 特别适用于处理复杂的知识问题。知识库中的具体内容如图 6 所示。

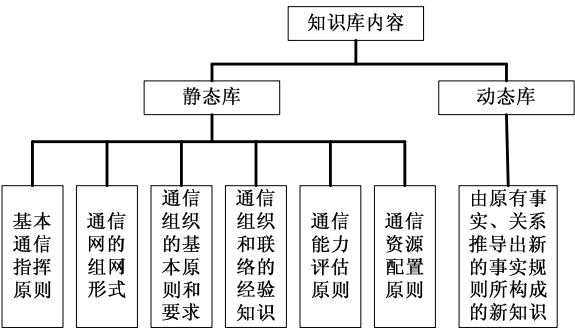


图 6 知识库中的内容

3.2.2 知识库中知识的表示

在野战中存在大量的不确定性因素，以选择通

信设备为例，在战场上，要根据地势、通信距离、所在地的频率等事实判断出所需通信设备的种类，以便选用不同的通信资源。根据军事知识的特点，我们采用两种知识表示方法。

① 基于规则的军事知识表示，例如：

RULE 1: IF 地势较起伏 and 远距离 and 保密通信 and 频率为 xxx-xxx MHZ  
THEN 采用某型战术卫星车载站 (0.7)

在军事知识的表示上，我们根据军事知识的特点和专家经验，给出知识的可信度因子 (0.7)，以此来解决不确定性的传递与合成等问题。

② 框架表示方法，例如：

(模板名: 通信距离  
范围: 从 0 到 10000 单位: 米  
模糊集合:  
(近距离 (Z 1000 4000))  
(远距离 (S 4000 10000))  
)

在这个描述中涉及到一些模糊语言如地势较起伏、远距离等，因此要结合相应的模糊数学的知识由相应的模糊集合 Z 形、S 形等进行表示。

3.2.3 知识库中知识的存储

通过以上的设计，我们采用关系数据库作为支撑来存储知识，依据知识库的表示方法，我们将知识库分为基于规则的知识库表示格式和基于框架的知识表示格式。

(1) 基于规则的知识表示格式

基于规则的知识表示中，规则的条件部分和结论部分都是由自然语言描述的，即都属于事实知识。我们根据所需军事知识的特点，如通信距离 >1000 米等，将事实看做是由一个表达式表示的知识，即将一个事实区分为事实前部 (通信距离)、事实中部 (>)、事实后部 (1000 米)。

同时，我们还规定如果某条规则的多个前提相互之间是逻辑“或”的关系，则在编辑知识时，应该将这样的规则拆分为几条相互独立的规则，而确保每条规则的所有前提之间都是事实的合取范式。

基于上述考虑，我们设计了事实库和规则库，各个字段的含义如表 1~表 3 中所示。



表 1 Facts（事实）表 结构

编号	字段名称	数据类型	含 义
1	事实号	int	对每一个事实给予一个自然数编号，此字段的所有值是以 1 为起始的连续自然数
2	事实左部	verchar	事实的自然语言内容，最多可存放 127 个汉字。规则左部、规则中部和规则右部共同描述一个前提或结论记录
3	事实中部	char	表示事实间的关系
4	事实右部	verchar	事实的自然语言内容，最多可存放 127 个汉字
5	可信度	int	0-1 之间的实数，初始时由专家给出，推理的过程中，将根据使用的频率和重要性计算

表 2 HeadRule（规则头）表结构

编号	字段名称	数据类型	含 义
1	规则号	int	区分规则的唯一标志。系统推理过程中，依据此编号来识别不同的规则，从而有效防止调度规则时发生混乱
2	适用范围	char	系统在推理过程中，依据此字段对规则分组，从而提高推理效率
3	规则前项数	int	条件部分所涉及的事实个数
4	规则后项数	int	结论部分所涉及的事实个数
5	可信度	int	0-1 之间的实数。冲突消减时，将根据可信度选取执行规则的顺序

表 3 Rule（规则）表结构

编号	字段名称	数据类型	含 义
1	序号	int	记录号
2	规则号	int	系统在推理过程中，依据此字段对规则分组，从而提高推理效率
3	规则属性	int	为 0 表示此记录为规则的条件部分；为 1 表示为规则的结论部分
4	事实号	int	代表所选中的事实
5	规则表示	int	代表该规则是否被用户确认为可用，只有当规则可用的时候才能作为推理的使用规则，这样可避免
6	知识解释	char	存放每条知识的解释文本的路径和文件名，若无解释，则为 non

(2) 基于框架的知识表示格式

我们设计了主框架库和槽库。主框架库用来存

储框架名称，槽库用来存储框架槽属性的具体值。  
各个字段的含义如表 4～表 5 中所示。

表 4 Frame（主框架）表结构

编号	字段名称	数据类型	含义
1	框架序号	int	框架唯一标示，此字段是以 1 为起始的连续自然数
2	框架名称	verchar	以自然语言的形式存储，最多可存放 127 个汉字
3	适用范围	char	系统在推理过程中，依据此字段对框架分组，从而提高推理效率

表 5 Slot（槽库）表结构

编号	字段名称	数据类型	含 义
1	序号	int	唯一标示
2	槽名	verchar	给出框架某一方面属性的自然语言描述
3	槽值	verchar	属性值，最终结果
4	框架序号	int	表明该槽是属于那个框架的

3.3 推理机

选取推理方法与系统知识的表示有直接的关系，为了提高推理效率，本系统设计有两大推理机：综合推理机，包括基于规则和基于框架的推

理；常用知识推理机只包括基于框架的推理。推理机流程如图 7 所示。当用户输入初始数据后，系统首先调用常用知识推理机，试图搜索当前情况最为匹配的情况，若有匹配的框架，则作相应的处理；否则，调用综合推理机，按照推理策略进行推理。

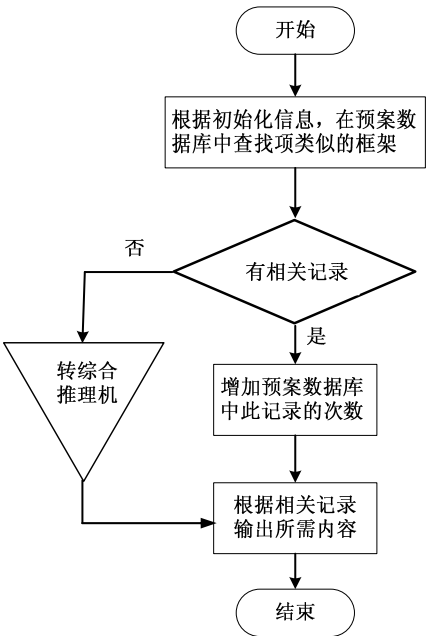


图7 推理机流程图

在每次调用常用知识推理机后，都会为预案数据库中访问的记录次数加 1，预案数据库按照访问次数递减顺序排列。这样，系统重复多次后，常用的知识将放在搜索的前列，从而提高了系统的效率。

在综合推理机中，无论是产生式规则推理还是框架推理都需从已收集的初始数据出发，按照一定策略，运用知识库中的知识，推断出结论，即采用正向推理。

3.4 评估模型

由专家系统形成的通信资源方案，往往不只一种，只有按照一定的指标体系，进行评估、排序才能得到最优的方案。在评估指标的选取上，我们根据总参《野战通信保障评估方案》将评估指标划分为业务指标和战术指标，从而对所形成的方案进行评估。具体指标划分见图 8。在每个细分的指标中，我们将根据各个指标的特点，建立数学模型。

例如在网络连通度上，我们利用网络的节点连通度概念来建立模型： $CN=\min[CN_{ij}]$ ，其中  $CN_{ij}$  为断开一对节点 (i, j) 之间所有通路所需去掉的最少节点数。

同时，我们还结合模糊综合评判的方法，对每一种具体的指标给出权重集  $W$ （从军事专家处获

取），即利用  $V=W\bullet F$ （其中  $\bullet$  表示模糊乘， $V$  表示评价指标， $W$  表示权重集， $F$  表示模糊变换矩阵），使得每一种指标根据在评估中所占的实际权重对通信资源配置方案进行评估。

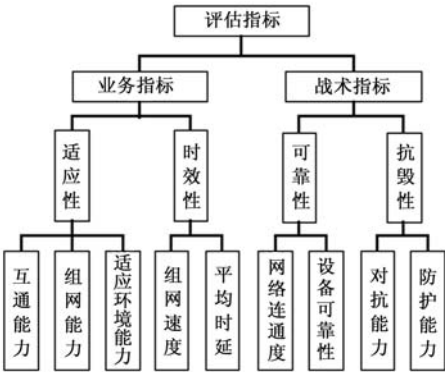


图8 评估指标体系

4 应用前景

智能化通信资源自动配置与评估系统从现存的通信状况和通信保障任务出发，以计算机为工具，借助专家系统和军事运筹等现代化技术开发而成，其根本目的是合理优化应用现有的各种通信资源，以便圆满完成受领的各种通信保障任务。系统使用对象既可为集团军（师）的通信指挥人员，又可为上级规划人员。其应用前景主要体现在以下两点：

(1) 应用价值

该系统能克服人工配制野战通信资源时考虑因素不周全、形成通信保障方案慢、缺乏灵活性等局限性，迅速生成数种可能的通信保障方案并进行比较优选。平时，该系统可用于军事训练，提高各级通信指挥员的指挥决策水平。战时，该系统可以为通信指挥员提供更精确的决策依据，提供更高級的“预测”能力，使通信指挥员可以争取更多的时间，不失时机地指挥部队行动。

(2) 理论价值

通过该系统生成的通信保障方案集合了一定的军事专家知识和实践知识，因此，可预测未来通信保障所需新通信资源的特征，同时对研究新的通信保障方案和军事理论有积极的作用。

5 结束语

本文就智能化通信资源配置与评估系统进行了

讨论,给出了系统的设计结构和实现方法,同时也显示了专家系统在军事领域的可行性和潜在的应用价值。在系统的研制过程中,随着对军事领域专家

知识的不断理解和完善丰富,该系统将获得不断进步和日益接近实战需求。

### 参考文献

- [1] 蔡自性,徐光佑.人工智能及其应用.北京:清华大学出版社,2003
- [2] 马鸣远.人工智能与专家系统导论.北京:清华大学出版社,2006.11
- [3] 胡桐清.人工智能.北京:军事科学院出版社,1999
- [4] 雷英杰,邢清华,王涛.人工智能(AI)程序设计(面向对象语言).北京:清华大学出版社,2005.10
- [5] (美) Joseph C.Giarratano Gary D.Riley. Expert Systems-- Principles and Programming (Fourth Edition).北京:机械工业出版社,,2006.8
- [6] (澳) Michael Negnevitsky. Artificial Intelligence --A Guide to Intelligence System (Second Edition).北京:机械工业出版社,2007.4
- [7] 蒋国庆.现代军队通信综合保障与新技术应用.武汉:国防科技大学出版社,2007.3

### 作者联系方式

通信地址:西安市王曲镇西安通信学院研究生管理大队九队

邮政编码:710106

联系电话:13319281368 029-84706443

# 信息资源开发利用对策思考

徐舸

**摘要：**我军信息资源开发利用基本形成了开发利用的环境，各种专用基础数据库初具规模，法规标准建设开始起步。我军信息资源开发利用主要存在“重硬轻软、重建轻用”的认识偏差，信息基础设施建设发展不平衡，信息资源开发利用标准体系尚未全面建立，信息安全防护漏洞较大等问题。为此，必须更新观念，提高认识；统一规划，分步实施；加强力量，完善机制；确保安全，提高效益。

**关键词：**信息资源；开发；对策建议

信息资源是指人类活动各个领域所产生的有使用价值的信息集合，与物质、能量并称为“三大资源”。信息资源除了具有其他资源相同的特征之外，还具有可数字化、方便复制、易于存储、传输快速和可以共享等特征。

军队信息资源开发利用就是在军队各项工作领域运用现代信息技术采集、处理、传递和使用军队信息资源，提升军队工作质量效能的过程。信息资源开发的任务是生成有用信息，通过信息的生产，来确保信息的供给。信息资源利用的任务是实现信息的价值，确保信息能够在军事活动中发挥作用，形成军事效益。信息资源开发是基础，信息资源利用是目的，二者互为因果，相辅相成。

## 1 我军信息资源开发利用的现状分析

随着我军信息化建设的快速起步和不断深入，军队信息资源开发利用逐步得到重视，各项工作开始起步，并初见成效。

### 1.1 我军信息资源开发利用取得的成绩

我军在信息资源开发利用方面作了不少工作，也取得一定成绩，主要体现在三个方面。

#### 1.1.1 信息资源开发利用的支撑环境基本形成

随着全军上下对信息资源开发利用的重视程度不断提高，以及各类信息系统的快速建设，对信息的生产、表示、整序、组织、存储、检索、重组、转化、传递、评价、应用等方面都提供了强有力的支撑，为全面深入开展信息资源开发利用提供了条

件，打牢了基础。

#### 1.1.2 信息资源开发利用的各种数据库初具规模

信息资源开发利用的各种专用基础数据库初具规模。各部门、各单位围绕平时训练任务和作战使命，在未来军事斗争准备的牵引下，开始建立敌情、我情和战场情况的相关数据库，初步能够满足作战、训练任务的完成。

#### 1.1.3 信息资源开发利用的法规标准建设开始起步

为了确保信息资源便于传输、交换与共享，建立全军通用的标准、格式至关重要。为此，全军信息化工作办公室制定并颁布了标准，总部相关业务部门也加快了相应法规标准的建设步伐，为信息资源开发利用工作健康快速发展初步创造了条件。

## 1.2 我军信息资源开发利用存在的问题

我军信息资源开发利用工作刚刚起步，就是相对于水平也不是很高的信息化基础设施建设来说，也相对滞后，是我军信息化建设中相对薄弱的环节，在一定程度上造成了“有硬件无软件、有软件无数据、有数据无共享、要共享无标准、有标准不执行、数据维护无机制”的现象。总体而言，我军信息资源开发利用主要存在以下四个方面的问题。

#### 1.2.1 “重硬轻软、重建轻用”的认识偏差是制约信息资源开发利用的首要因素

信息资源开发利用之所以滞后于军队信息化建设，主要还是思想认识问题。特别是重硬轻软思想

比较突出、重建轻用问题十分普遍。近些年来,部队自行开发建设的野战指挥系统、作战指挥中心、信息网络,硬件档次越来越高,但相应的应用软件没有跟上,使已建硬件设施效能得不到充分发挥,使得信息资源的开发利用没有依托。大量的计算机主要用于打印显示浏览文字、图表,急需的战术作业、辅助决策功能难以实现,即使积累了一些信息资源,也难以在没有应用软件的系统里发挥作用。一些部队舍得投入搞建设,但不愿花钱抓应用,个别的甚至搞了一些建为看的“门面工程”、建为演的“观摩工程”、建为奖的“入库工程”。许多单位建成了信息系统之后,没有人搞数据维护,搞信息更新,没有着眼当前打基础,立足长远抓积累,而是需要一点建一点、想到一点设一点,而且还缺乏继承性,对以前建设的项目继承的少、摒弃的多,有的甚至全盘推翻,重复建设、反复投资现象比较突出,资源浪费非常严重,信息系统运用中“最后一公里”现象十分突出(在信息系统的最末端,缺少数据采集、维护这个环节,造成整体功能的缺失)。尽管这些系统能够完成一些信息资源开发利用的功能,但因缺少相应的数据,就造成了这些系统不能真正走入应用,也不能检验系统性能,促进系统功能的完善与改进。当前,我军在建和已经建成的数据库数量、种类都非常多,但都不够完善,要么数据库没有完整可用的数据,要么数据库内数据因长期得不到更新而过时失效;对已开发的数据缺乏疏理、加工和优化,使多数信息停留在文字和表格上,难以完成实时传输、实时控制功能;许多系统用于进行作战数据计算、优化和评估的信息资源太少,使计算机辅助决策由于缺少相应的信息资源支撑,成了“巧妇难为无米之炊”,长期停留在较低水平上;有的参谋人员不善于使用信息系统,学习计算机知识仅仅满足于会打字,把电脑简化为打字机和存储器,信息资源开发利用的主动性不够的情况比较普遍。从以上现象可以看出,思想认识上的偏差是制约信息资源开发利用的首要问题。

### 1.2.2 信息基础设施建设发展不够平衡一定程度上限制了信息资源的开发利用

军事信息基础设施主要包括各种侦察监视预警探测系统、指挥信息系统、计算机数据库、军队日常业务工作平台、信息安全防护设备、与武器系统交链的数据链系统、用于信息传输的各类通信网络等。目前,在侦察探测方面,对低空小信号及隐身

目标的发现能力仍较弱;在指挥信息系统建设方面,缺少全军统一的系统,互联互通性能比较差,难以满足一体化联合作战需要;在计算机数据库和军队日常办公信息系统建设方面,多数系统还是各自单位自行建设,自成一体,不能与外部互联互通,且即时更新、扩展不够;在数据链建设方面,三军统一的通用系统还未建成,与现有的各军种作战软件交链融合不够,难以很快形成作战能力;在通信信道建设方面,发展也很不平衡,很多单位的通信手段还相对落后,信息传递手段比较单一。信息基础设施建设的这些薄弱环节,直接导致了信息资源开发利用受到了诸多限制,比方说,情报信息的来源相对较少,信息的生产受到限制;信息系统的功能不够完善,信息资源开发利用也就缺少正确的需求牵引,难以达到理想的效果;各种信息系统互联互通性差,信息资源开发利用也就难以做到充分共享,等等。可以说,信息基础设施建设是军队信息化建设的基础,也是信息资源开发利用的基础。

### 1.2.3 信息资源开发利用标准体系尚未全面建立直接制约了信息资源的交换与共享

军队信息资源的开发必须在统一的技术体制和标准下进行,这是实现信息资源利用和共享的基础。我军在这方面已经作了一些工作,但差距还非常大。由于军事信息资源开发利用缺乏相对统一的信息标准,加上各单位开发方法不统一,特别是缺乏跨领域、跨部门统一的信息编码体系结构和国防数据字典系统,军事信息资源开发利用存在着规范性和唯一性不强、各自为政等缺点,没有很好的依据标准进行数据源建设,使人与人之间、人与机器之间以及机器与机器之间、系统与系统之间不能够无障碍,不失真地进行沟通和交换信息,信息资源在互联互通互操作方面存在明显问题,直接影响其作用效益发挥。比如,有的单位投入几十万甚至上百万元的资金搞信息系统建设,虽搭建起了不少“烟囱”,但由于自身建设的局限性,无法互联互通,更谈不上与武器系统交链,而用于自身内部交换的信息又不多,仅仅实现一个营院或一个大楼的自动化,显然与作战需求和作战使命相去甚远,既发挥不出计算机网络的信息交互优势,又占用了本来就十分有限的战备训练经费,影响了部队战备训练的正常进行。

### 1.2.4 信息安全防护漏洞大给信息资源开发利用工作带来较大隐患

在信息化程度不断提高的军队中,信息安全是军事安全,乃至国家安全的重要组成部分,也是信息资源开发利用的首要问题。从我军的实际情况看,信息安全防护存在先天不足,我国在以计算机、通信和网络技术应用和不断升级的信息产业核心技术领域都不占优势:在硬件上,微处理器、骨干路由器等基本上都依赖进口;在软件上,计算机操作系统、网管软件等基础性软件几乎都是外国的产品;具有自主知识产权的高性能的作战模拟算法几乎是空白。这些缺项和弱点,严重影响了我军信息化建设的质量与安全。当前,由于我军现有信息网络的安全保密管理还存在不少问题,在信息资源的开发利用中“有网不敢用、不放心”,给开发利用的深入发展带来了很大困难。军队信息资源具有很强的保密性,信息资源的使用和共享,必须在安全保密的前提下进行,否则就会适得其反。同时,有些单位、有些部门信息安全意识淡薄。对有形的秘密载体管理得非常严格,对无形信息的安全保密管理没有有效措施,甚至放任自流,通过信息传递造成的失泄密问题仍然比较严重。在早期信息系统建设中,安全保密问题考虑较少,客观上造成信息资源的安全性能不够,这也给信息资源开发利用带来较大隐患。目前,我军信息资源得不到有效开发利用的一个重要原因,就是信息系统安全漏洞大的问题还没有解决好。

## 2 我军信息资源开发利用的对策思考

军队信息资源开发利用是一项长期、艰苦的工作。积极推进我军信息资源开发利用既是建设信息化军队、打赢信息化战争的客观要求,也是提升现实作战能力,做好军事斗争准备的迫切需要。依据信息化建设的发展大势和我军实际情况,应重点做好以下四个方面的工作。

### 2.1 更新观念,提高对信息资源开发利用的认识

在信息时代,信息资源对于作战双方的重要性在于谁掌握的信息更全、更多、更快、更准、更新,谁就更有获胜的基础;谁对信息应用的效率更

高、效果更好,谁就更有取胜的保证。在信息化建设中,信息资源是发挥高技术武器装备性能的“粘合剂”,没有信息资源的开发利用,搞信息化建设就等于无源之水、无本之木,信息设施离开信息资源就不会有存在的价值。只有把信息资源通过完善的信息系统和信息网络进行高效互通并与武器系统有效交链,才有达成联合作战信息优势的可能,从而为赢得战争的胜利打下基础。因此,在推进信息资源开发利用中,必须确立三个观念。

#### 2.1.1 信息制胜的观念

切实认清信息就是战斗力,信息资源就是最重要的战争资源,把信息资源开发利用置于提高打赢能力的战略高度,抓好全面落实工作。未来信息化条件下的海上战争,信息资源既是信息进攻的重要手段,也是信息进攻的主要目标,同时也是信息防御的核心。当代局部战争的实践证明,谁掌握了大量的有价值的信息资源,谁就掌握了制信息权和战争的主动权,谁就能打赢战争。

#### 2.1.2 信息共享的观念

信息的最大优势就是便于共享,只有在充分共享中才能发挥最大效益。但在机械化战争的传统观念中,条块分割、自成体系的做法,是不能适应信息资源开发利用工作的。只有树立“信息共享”的观念,在会以统一的标准格式开发信息,才能积极主动地建立信息交换协调机制,把不同部门、不同单位,甚至是民用信息资源开发利用统一起来,充分发挥整体信息优势,尽快提高信息资源开发利用的工作效益。

#### 2.1.3 需求牵引的观念

打什么仗,就建设什么样的军队。军队建设的首要问题就是搞清需求、明确方向。信息资源开发利用更是如此,信息资源的内容、格式、存储方式、传输流程都需要作战需求的牵引。需求不清是我军信息化建设的薄弱环节,也是信息资源开发利用的薄弱环节。必须把需求论证放在重要战略位置,建立稳定的需求研究队伍,加强三军联合作战信息资源开发利用总体需求论证,特别是要在量化、细化、具体化上下工夫,提高需求的可操作性和指导性,确保我军的信息资源开发利用工作能够有正确的目标、明确的方向。

## 2.2 统一规划，打牢信息资源开发利用的基础

信息资源开发利用是个庞大的系统工程，必须要在统一的规划和组织下，才能形成合力，加快发展。首先要坚持自上而下的原则，搞好顶层设计，打牢发展基础。顶层设计最为重要的是要有信息资源的宏观规划，每个单位要在上级的统一规划下，确定自己的信息资源开发利用框架结构。同时，要制定信息资源开发利用的法规和标准，明确各部门、各单位在信息资源开发利用中的责任，明确协调共享机制，确定数据格式和接口规范，保证各部门、各单位的信息资源开发利用工作是在统一规划和标准下进行的，为信息系统的综合集成，为一体化信息系统的建成打下坚实的基础。此外，信息资源开发利用是一项长期任务，不能一蹴而就，也不是一朝一夕的事情，必须从基础做起，逐步积累完善。当前，要紧贴现实军事斗争准备之急需，建立作战资料分类数据库，增加基础数据和动态数据的储备量，并及时进行动态更新。要建立作战模型数据库，根据不同的作战方案和作战模型，与作战资料数据库相联，能计算生成多种作战计划和战法，为指挥员提供辅助决策建议。要建立三军通用的指挥作业和态势软件，使三军情报能够融合，三军作战态势能够合成，确保联合作战行动顺利实施。

## 2.3 健全机制，保证信息资源开发利用的顺利开展

信息资源开发利用在信息化建设中的突出地位，要求我们必须加强力量，加大投入，加速信息资源开发利用发展。要承认信息资源开发利用的价值和工作量，舍得投入。要增加信息资源开发利用经费，作为各单位信息化建设或日常工作经费的一部分专款专用，保证信息资源开发利用工作的顺利开展，保证数据工程建设能够尽快起步、顺利实施。其次，要增加一定数量的信息资源开发利用专职人员。尽管信息资源开发利用贯穿到军队活动的方方面面，不同单位、不同业务部门的人员都有职责参与到这项工作中，但信息录入、整理、分析和处理工作量大，需要人员多，必须有一定数量的专职人员从事这项工作。地方的一些信息中心和网站，都有大量的信息开发人员。在经费、人员落实

之后，最为重要的就是建立机制。信息资源开发利用工作重点要建立四项机制。

### 2.3.1 数据更新机制

要不断更新数据库，确保提供给用户的是最新、最准确的数据；建立健全数据访问机制，为实时更新数据库提供技术支撑。

### 2.3.2 数据共享机制

要站在军队建设全局的高度，制定规章制度，建立日常的信息交换机制，公共信息资源必须全面共享。为此，必须在以下几个方面的关键问题上，达成共识：共享与交换信息服务对象的问题，不同的服务对象应采用的服务方式问题，共享信息的存储与统一管理问题，对信息的来源怎样进行科学分析，相应的信息技术标准与管理标准问题，信息交换与共享平台的设计与建设应遵循的原则等。这些问题是解决信息交换与共享的核心问题，无论解决信息交换与共享的技术方法如何不同，这些问题一直是解决信息资源开发利用的基础和保障。

### 2.3.3 数据融合机制

多信息元素、多信息源、多手段、多目标数据融合是数据信息融合的最大特点，也是最大难点。多信息元素包括态势、文字、图像、声像、语音等信息；多信息源来源于航天、航空、海上、岸基等多个侦察和探测系统；多手段包括通信信号侦察、非通信信号侦察、遥感侦察、光电侦察、网络侦察、群众侦察、谍报侦察、雷达探测、水声探测等手段获得的信息。总之，由于信息表现形式的多样性、信息数量的巨大性、信息关系的复杂性、信息处理的及时性特征，使数据融合机制的建立更具有迫切性。

### 2.3.4 日常应用机制

开发的信息资源只有在应用中才能发挥作用，要鼓励各单位用新技术、新方法、新手段来研究问题、处理工作，要强制性地推广网上作业、无纸化办公、智能化管理等工作制度，有条件的部队和单位，应建立局域网和远程办公系统，提高信息利用的效率。使信息资源开发利用工作在实际应用中，不断完善，良性发展。

## 2.4 确保安全，提高信息资源开发利用的效益

安全保密是信息资源开发利用的首要保证，没有安全，信息资源就不可能发挥效益，甚至是反面效益。但是，共享和安全保密又是一对不可回避的矛盾。首先，信息资源开发利用的根本是实现信息资源共享，信息资源得不到有效共享就体现不出信息资源开发利用的价值和信息系统的作战效益，因此，信息化建设必须要一体化建设，真正达到系统互联、互通、互操作。但是，共享又在一定程度上给安全保密造成了隐患，给自己方便的同时，也可能给敌人造成可乘之机。我们的信息安全保密工作并不是非常理想，我们的长城网就曾经遭到境外的攻击、还有一些军用涉密计算机私自接入互联网、

许多安全防护措施落实不到位等等。因此，必须强化安全保密意识，要确保信息资源在安全保密的前提下发挥效益；要充分发挥机要、保密部门的职能作用，强化信息资源安全保密的监督管理；要确保军事信息网络与国际互联网的物理隔离，这是目前信息安全管理最有效、最可靠的办法；要切实落实数据加密、加装防火墙等安全保密措施，严格管理制度，做到防患于未然；要加强对自主知识产权设备的应用，提高信息安全保密的主动权。总之，我们要采取一切措施确保信息资源开发利用的安全可靠，确保在安全保密的前提下提高信息资源开发利用的效益。

### 参考文献

- [1] 《关于加强信息资源开发利用的几点意见》. 中办发（2004）34号
- [2] 《军事信息化：整合信息化资源之我见》. 解放军报，2003年12月10日
- [3] 戴清民. 《军队信息资源开发利用的几个问题》，2006年11月
- [4] 王保存. 外军信息资源开发利用的主要做法. 北京：《国防》2006年02期

### 作者联系方式

通信地址：海军指挥学院信息战研究系

邮政编码：210014

联系电话：13701460818



# 获取领域知识的本体体系结构的构建

许勇 王智学 李宗勇

**摘 要:** 为了准确完备地获取领域知识,并使之成为需求工程中各方人员普遍接受的规范,本文提出了一种基于本体的领域知识获取方法。该方法的主要特点是:利用具有不同抽象程度的本体组成的体系结构来获取和复用领域知识,利于保证知识获取的完整性和一致性。文章首先提出了业务本体、领域本体和应用本体的三层体系结构,利用该体系结构来获取和复用领域知识;接着采用具有形式化语义的 OWL DL 语言对本体进行描述,规范本体的语法和语义;最后,对本体进行推理,检查本体内部的一致性。

**关键词:** 需求工程;军事电子信息系统;本体;领域复用;OWL

## 1 引言

软件产品的生产可以看成是一个映射,将客户最初的非形式想法映射成最终解决此问题的软件产品,需求工程则是这一巨大飞跃中起决定性作用的第一步,需求工程的质量的好坏对项目的成败有着至关重要的影响。然而,需求工程是一个相当复杂的过程,它所面对的问题几乎没有范围,应用的领域非常广泛,它的实施与各个应用行业的特征密切相关,并且它需要方方面面的人员的参与(如领域专家、领域用户、系统投资人、系统分析员、需求分析员等等),各方面人员有不同的着眼点,不同的知识背景,沟通上十分困难,常常造成对统一目标系统的不同认识,形成所谓的“通信鸿沟”。如何确保需求工程的质量是需求工程中一个十分重要的问题。

在需求工程的早期阶段对问题领域进行建模和分析,对成功实施需求工程非常关键,这一观点正逐步成为需求工程领域的共识<sup>[1-3]</sup>。而对问题领域进行建模和分析,实质上就是领域知识获取的过程。只有在各方面人员对于领域知识有着共同理解的前提下,才能保证相互之间沟通顺利,才能形成对同一目标系统的共同认识,才能保证获取的需求的正确性。如果能够统一知识的组织和表达,使之成为领域内各方面人员普遍接受的规范,就有可能解决知识共享的问题,有效地消除通信鸿沟。而且,在相同或相似的领域中,不同的应用往往涉及到相同的领域知识,如果能够抽取出这些领域知识,用统一的形式加以表达,就能在相同领域中的

不同应用之间很好地进行复用,从而避免重复的领域知识分析,提高领域分析的效率和准确性。

基于知识,特别是基于本体的方法是目前研究较多的一种方法,它试图利用本体在知识表示方面形式化、规范化的优势,解决领域内知识共享的问题;利用本体作为领域中重要实体、属性、过程及其相互关系形式化描述的基础的特性,解决领域内知识复用的问题。本文提出了一种基于本体的领域知识获取和复用的方法,它通过一个三层的本体体系结构来引导领域用户全面描述现实系统,来达到对领域知识的共享和复用。

## 2 相关知识介绍

军事电子信息系统需求描述语言(MEISRDL)<sup>[4]</sup>是军事电子信息系统需求模型的建模基础语言,它提供了一种对需求的通用描述框架,分别从业务、技术和功能操作三个方面来对系统的需求进行描述和规约。其中业务框架是系统中最为关键的部分,军事人员在业务框架的引导下阐述他们的业务概念以及对信息系统的要求,在框架引导下将业务需求映射为对业务概念各特征的描述实例,构成了容易被技术人员所理解的业务概念模型,进而形成了双方共识的、较为准确的问题领域背景知识。

## 3 方法概述

本文在军事电子信息系统需求描述语言的基础上,对业务框架进行丰富,提出了一个业务本体、

领域本体和应用本体的三层体系结构，在这个三层体系结构的指导下来获取具体领域知识，其主要思想是：① 业务本体作为描述业务的元模型，从九个方面规范和系统化业务描述，保证业务描述的完整性。② 领域本体是业务本体在具体领域的实例化，包含了特定领域的可重用的概念、概念之间的关联以及相关的约束。③ 应用本体是用户在业务本体的引导和领域本体约束下对具体应用的描述，也就是对具体领域知识的描述。这种方法的优点是：各本体具有不同的抽象程度，下层本体的建立可以得到上层本体的引导和约束，从而保证领域知识获取的完整性和一致性。该方法的总体结构如图 1 所示。

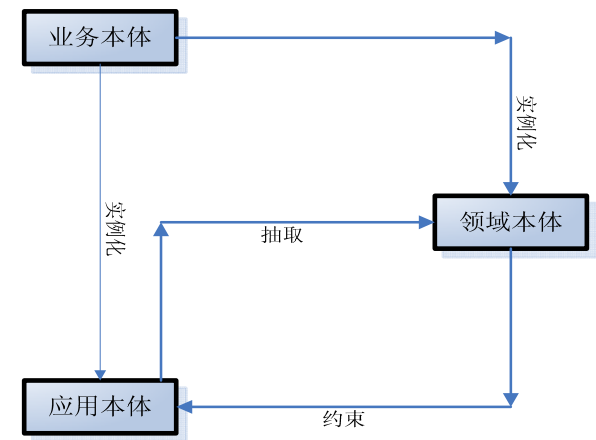


图 1 基于本体的领域知识获取

由图可以看出，业务本体作为顶层本体，规范了对业务的描述。需求分析人员与领域用户在业务本体的引导下进行交流和讨论，通过实例化业务本体中的相关元概念和关联得到具体应用的描述，即应用本体；对信息技术和领域知识都有所了解的知识工程师在业务本体的引导下，将在领域内通过业务本体实例化而又不依赖于具体应用的概念和关联等组合在一起形成领域本体。因此领域本体可以在同一领域进行复用，同时也可以约束领域内相关应用本体，指导应用本体的建模；反过来通过抽取应用本体又可以丰富领域本体。

本文下面几节分别介绍该本体体系结构中的不

```
<?xml version="1.0"?>
<!DOCTYPE rdf:RDF[<!ENTITY xsd "http://www.w3.org/2001/XMLSchema#">.....]>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:rdf="http://www.w3.org/2000/01/rdf-schema#"
xmlns:owl="http://www.w3.org/2002/07/owl#"
xmlns="http://www.owl-ontologies.com/unnamed.owl#"

```

同成分，以及它们的形式化描述。

4 业务本体

4.1 抽象语法

定义 1：业务本体定义如下：

```
Business ::= (< BusName >,< BusConS >,< AttBusConS > ,
< BusConAssS >,< AttBusConAssS > )
```

其中，<BusName>是业务本体的名字，即：BusinessOntology，<BusConS>是业务本体中概念的集合，包括局面、职能、目标、政策、行为、角色、结果、资源和环境。而角色又分为人、机构和系统。<AttBusConS>是业务本体中概念属性的集合，<BusConAssS>是业务本体中关系的集合，<AttBusConAssS>是业务本体中关系属性的集合。

关于业务本体中各个概念的详细描述，这里就不作具体介绍了，详细定义见军事电子信息系统需求描述语言<sup>[4]</sup>。概念之间的关系如图 2 所示。

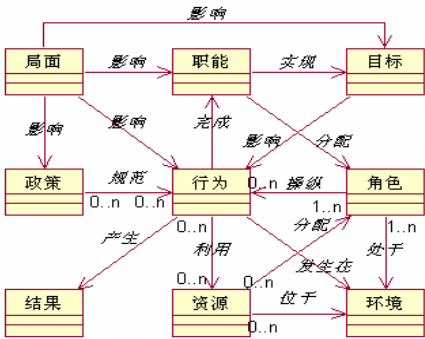


图 2 业务本体中概念间的关联

4.2 具体语法描述

OWL 是 W3C 推荐的语义 web 本体的描述语言，它有三个子语言：OWL Lite、OWL DL 和 OWL Full。本文采用基于描述逻辑的 OWL DL 子语言，其有丰富的表达能力，并且具有可判定的推理能力<sup>[5]</sup>。以下是对业务本体的部分描述：

```

xml:base="http://www.owl-ontologies.com/unnamed.owl"
<owl:Ontology rdf:about="">
<rdfs:comment>业务本体</rdfs:comment>
<rdfs:label>Business Ontology</rdfs:label>
</owl:Ontology>
<owl:Class rdf:ID="Role">
  <rdfs:comment>participator of a business</rdfs:comment>
  <rdfs:label>Role</rdfs:label>
<!--限制属性 RoleName 的值唯一-->
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty rdf:resource="#RoleName"/>
      <owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1
      </owl:cardinality>
    </owl:Restriction>
  </rdfs:subClassOf>
</owl:Class>
<!--限制属性 RoleName 的值为字符串-->
<owl:DatatypeProperty rdf:ID="RoleName">
  <rdfs:domain rdf:resource="#Role"/>
  <rdfs:range rdf:resource="&xsd:string"/>
</owl:DatatypeProperty>
<owl:Class rdf:ID="Human">
  <rdfs:subClassOf rdf:resource="#Role"/>
</owl:Class>
<owl:Class rdf:ID="System">
  <rdfs:subClassOf rdf:resource="#Role"/>
  <owl:disjointWith rdf:resource="#Human"/>
</owl:Class>
<owl:Class rdf:ID="Organization">
  <rdfs:subClassOf rdf:resource="#Role"/>
  <owl:disjointWith rdf:resource="#Human"/>
  <owl:disjointWith rdf:resource="#System"/>
</owl:Class>
<owl:ObjectProperty rdf:ID="effect">
  <rdfs:domain rdf:resource="#Situation"/>
  <rdfs:range>
    <owl:Class>
      <owl:unionOf rdf:parseType="Collection">
        <owl:Class rdf:about="#Objective">
          <owl:Class rdf:about="#Functionality">
            <owl:Class rdf:about="#Activity">
              <owl:Class rdf:about="#Policy">

```

```
</owl:unionOf>
</owl:Class>
</owl:range>
</owl:ObjectProperty>
.....
</rdf:RDF>
```

在上述代码片断中，简单定义了业务本体中的角色概念，限制了角色名是唯一的，并且为字符串类型；定义了角色的三个子类：人员、系统和机构，它们三个是互不相交的；定义了影响关系，它的定义域是局面，值域是目标、功能、活动和政策。

5 领域本体

在相同或相似的领域中，不同的业务所要实现的具体目标、所担负的具体任务和所处的环境等都有明显的差异，因此它们的操作流程会有所区别。但是它们往往涉及到领域内的一些公认的概念和术语，它们具有领域通用性，因此如果抽取出自领域中的这些与应用无关或与具体任务无关的领域知识，并将其进行规范化的描述。在对这些领域经过验证和确认后，便可以在同一领域中的不同业务之间达到很好地复用，并能很好地指导应用模型的建立。由于本文中领域本体受业务本体的约束，并且强调领域本体应与具体任务和流程无关。因此在领域本体中只涉及到业务本体中的人员、系统、机构、资源和结果五个方面，即领域本体中的概念的父类是人员、系统、机构、资源或结果中的一种。

定义 2：领域本体定义如下：  
Domain ::= (< DomName >,< DomConS >,< AttDomConS >,< DomConAssS >,< AttDomConAssS >,< DomAxis >)

其中，<DomName>是领域本体的名字，<DomConS>是领域本体中的概念的集合，<AttDomConS>是领域本体中概念属性的集合，<DomConAssS>是领域本体中概念关系的集合，<AttDomConAssS>是领域本体中概念关系属性的集合，<DomAxis>是领域本体中公理的集合，包含的是领域知识中的一些永真断言，比如：概念之间的继承、等价和不相交，以及属性之间的继承、等价。

下面，以一个简单的卫星侦察领域本体为例来

进行说明（该例子只是起示范作用，并不具备实际意义），如图 3 所示。

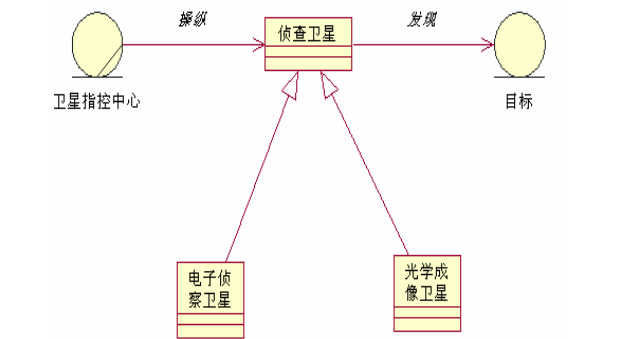


图 3 卫星侦察领域本体

其中，概念集如表 1 所示。

表 1 概念集

概念标识	概念名称	概念类型	约束
O-01	卫星指控中心	机构/角色	
S-01	侦察卫星	系统/角色	
S-02	电子侦察卫星	机构/角色	
S-03	光学成像卫星	机构/角色	
RT-01	目标	结果	

概念之间的关系集如表 2 所示。

表 2 概念之间的关系

标识	关系名	定义域	值域	类型	约束
RA-01	操纵	卫星指控中心	侦察卫星	Association	
RA-02	子系统	电子侦察卫星	侦察卫星	Generalization	传递性
RA-03	子系统	光学成像卫星	侦察卫星	Generalization	传递性
RA-04	发现	侦察卫星	目标	Association	

领域本体具有两个重要作用：① 启发，在需求获取中可以通过重用领域概念获得对应用本体的描述；② 约束，领域本体定义或限定了应用本体的语义，为应用模型的推理验证奠定了基础。

## 6 应用本体的描述

定义3: 应用本体定义如下:

$Application ::= (< AppName >, < AppConS >, < AttAppConS >, < AppConAssS >, < AttAppConAssS >, < AppRulS >)$

其中,  $<AppName>$  是应用本体的名字,  $<AppConS>$  是应用本体中概念的集合,  $<AttAppConS>$  是应用本体中概念属性的集合,  $<AppConAssS>$  是应用本体中关系的集合,  $<AttAppConAssS>$  是应用本体中关系属性的集合,  $<AppRulS>$  是应用本体中规则的集合, 它包括一些个体类型的断言, 个体之间的关系的断言以及具体应用中所声明的一些规则。

## 7 基于本体体系结构的领域知识获取过程

领域知识的获取的过程实际上就是建立应用模型的过程, 它的步骤如下。

1) 业务本体作为描述领域知识的一个总的框架, 军事领域专家或知识工程师在它的引导下, 在图形化工具的帮助下, 描述相关领域内可复用的概念、概念间的关系以及约束的集合, 从而得到相应的领域本体, 并导出到领域本体库中。这里的概念主要是一些静态的概念, 也就是上面所提到的角色、资源和结果三个方面。图形化工具采用的是项目组开发的信息系统需求获取工具<sup>[4]</sup>。

2) 从领域本体库中导入相关的领域本体。

3) 需求分析人员与领域用户在业务本体的框架制导下进行交流, 通过实例化业务本体中的概念获取应用本体中的个体, 把应用本体中有关角色、资源和结果的静态个体与领域本体中的相关概念建立联系, 在领域本体的启发和约束下建立完整的应用模型。

4) 如果应用本体中出现新的类型的个体或者新的关系类型, 而领域本体中没有对应的概念或关系, 则从应用本体中抽取出这些概念或关系加入到领域本体中, 对领域本体进行丰富。

应用本体是对系统需求模型相关要素的抽象描述, 获取应用本体的过程也是需求获取和分析的过程, 在获得完整的应用本体之后可以通过一定的技术将其自动转换成应用软件模型<sup>[6]</sup>。

## 8 结论

本文以军事电子信息系统为研究背景, 在军事电子信息系统需求获取语言的基础上提出了一种业务本体、领域本体和应用本体的三层体系结构, 以此来获取和复用领域知识。目前在军事电子信息系统需求获取工具<sup>[4]</sup>中已经对业务本体和应用本体实现了图形化表示, 但是对于领域本体而言, 它的图形化表示还有待进一步细化; 而且对于具体的领域内的演绎推理规则如何表示, 如: 如果教师甲编写了教材乙, 课程丙使用了教材乙, 那么必须要求教师甲来教授课程丙; 该方法也没有涉及到, 这些都成为下一步的研究方向。

## 参考文献

- [1] Lamsweerde A V. Requirements engineering in the year 00: A research perspective, In: Proceedings of the 22nd International Conference on Software Engineering, Limerick, Ireland. 2000.5~19
- [2] Yu E. Towards modeling and reasoning support for early-phase requirements engineering. In: Proceedings of the 3rd IEEE International Symposium on Requirements Engineering, USA, 1997.226~235
- [3] Haumer P, Pohl K, Weidenhaupt K. Requirements elicitation and validation with real world scenes. Technical Report CREWS Report, 98-06. Germany, 1998
- [4] 王智学. 一种业务概念模型驱动的需求分析与获取方法[J], 军事运筹与系统工程. 2006, 20 (1): 18~22
- [5] W3C. World Wide Web Consortium Issues RDF and OWL Recommendations[EB/OL]. <http://www.w3.org/2004/01/sws-pressrelease.html.en>, 2004-02-10.
- [6] 金芝. 基于本体的需求自动获取, 计算机学报. 2000, 23 (5), pp.486-492.

## 作者联系方式

通信地址: 江苏省南京市海福巷1号指挥自动化学院研究生一队 邮政编码: 210007 联系电话: 13770609674

# 基于信息融合的装备保障多目标群决策支持系统研究

颜宁 周巍 朱晓华

**摘 要:** 针对作战需求, 综合集成军事运筹、系统分析、信息融合、决策支持和人工智能等边缘学科理论和信息处理、网络通信、多媒体等现代技术, 将战场态势评估、军事情报分析、数据挖掘技术和地理信息系统、信息管理系统等有机结合, 提出了一种多层次、智能化的多目标、群决策、分布式信息网络支持系统, 可为装备平时使用管理和战时保障指挥决策提供技术支持, 为进行装备保障规划、资源优化配置、保障行动部署和下定保障决心提供了有效的技术手段。

**关键词:** 多目标决策; 群决策; 决策支持系统; 信息融合; 人工智能; 装备保障

## 1 引言

以信息化为先导的科学技术的迅猛发展及其在军事领域的广泛应用, 促使一大批高技术武器装备相继问世并广泛用于战争, 深刻地改变了战争的全貌, 从战争形态到作战样式, 从作战指挥到技术保障, 都出现了前所未有的高技术特征。战场变化的急剧性, 战争时空的整体性, 作战手段的多样性, 使装备建设工作所面临的新情况、新问题、新矛盾层出不穷, 对装备保障的要求越来越高, 依赖程度也越来越大, 装备保障作为提高部队战斗力的一种有效手段, 已逐步发展成武器装备建设链条中的关键环节, 成为影响战争进程和结局的重要方面。

未来高技术战争是体系与体系的对抗, 装备保障更突出全局性、战略性和系统性。由于现代高新技术的发展和应用, 促使武器装备的射程、威力、精度都几乎达到了各自的极限, 交战双方的差别在很大程度上取决于他们对作战及其保障的指挥控制和决策的水平上。要在现代化信息条件下完成作战任务, 不但要在武器装备、指挥控制方面重视信息化建设(例如, 数字化部队, C<sup>4</sup>I 系统等), 还必须重视信息技术在装备保障领域中的应用研究。如何在信息作战条件下, 充分利用信息技术, 实现保障资源的优化管理与信息共享, 提高装备保障能力, 已成为亟待解决的重要课题。

本文针对战时装备保障的实际需求, 以军事运筹学、系统分析、信息融合、决策支持和人工智能理论为基础, 以网络通信、信息处理、多媒体等现代技术为支撑, 以目前较成熟的专用网络平台为依托, 构建了一套具有实时性、直观性、交互性和集

成性的多层次、全方位、数字化的多端信息网络支持系统。从情报信息融合、目标威胁判断、战场态势评估、保障方案的合理选择、保障资源的统筹规划、保障指挥的决策与控制以及各保障要素之间的协同等方面, 对装备保障的决策过程进行了深入的研究和系统的分析。该系统将决策支持系统与地理信息系统、信息管理系统有机集成, 能够综合处理各类信息, 实现保障信息的显示和查询以及保障方案的动态变化, 达到推演战场态势、制定保障方案、调动保障资源的目的。整个装备保障的决策过程可自动地或人机交互式地进行, 使得装备保障的指挥决策更加科学化、自动化、智能化。

## 2 系统的体系结构

保障决策是一项综合性很强的系统工程, 相应的决策支持系统是一个宏观与微观决策相混杂的庞大而复杂的系统, 它既有一般的指挥决策与控制、信息网络系统的普遍规律, 也有对装备实施综合保障(特别是战时)所提出的特殊要求。为实现保障决策, 决策支持系统由硬件环境和软件环境装备两大部分组成。

### 2.1 硬件组成

硬件环境是保证系统在硬件上达到分布式环境和多媒体环境的设备。本文所设计的支持系统是一个开放的分布式多媒体通信集成环境, 以专用通信网络为依托, 以较为完善的各级内部局域网为基础, 采用分布式多层结构, 主要由计算机设备(包

括用户终端计算机和网络服务器)、成套的多媒体设备(包括音频输入输出设备、视频输入输出设备、CD-ROM等)、网络及远程通讯设备(网卡、集线器、屏蔽双绞线等)、计算机输入输出设备、数据传输设备等组成,系统的网络拓扑结构如图1所示。

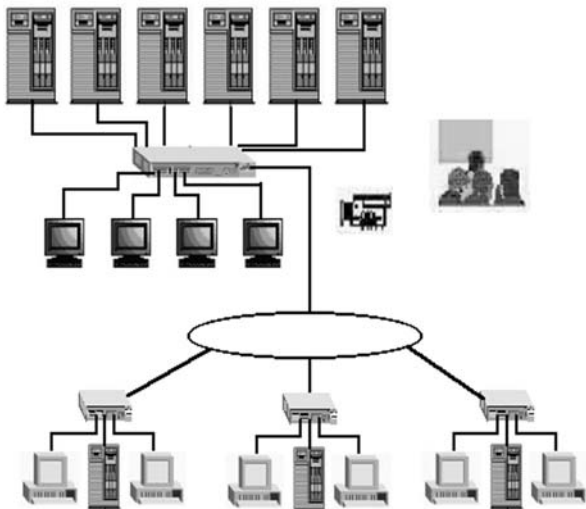


图1 系统的网络拓扑结构

2.2 软件组成

采用面向对象的方法设计出分布式的多媒体智能辅助决策支持系统。各种信息的获取和对战场态势的评估是遂行装备保障指挥的基本前提。因此,装备保障决策支持系统除了具有一般的决策支持系统所包含的功能外,还应包括情报信息处理系统、战场态势评估系统、地理信息系统以及信息综合管理系统。其总体结构如图2所示。

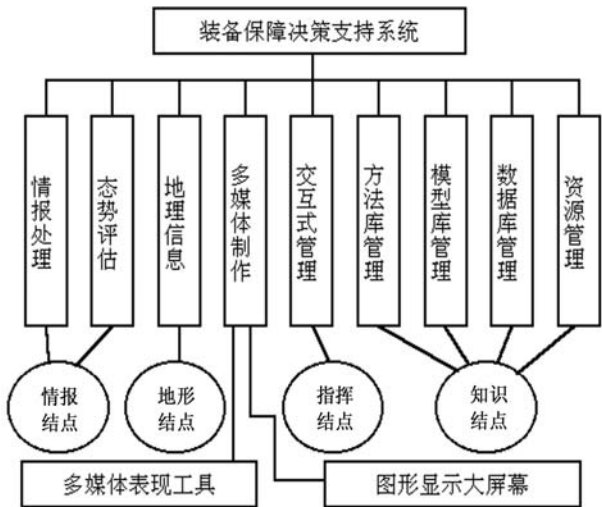


图2 系统的软件结构

3 系统设计

装备保障决策支持系统是一个能够帮助决策者利用数据、模型,解决半结构化问题、以计算机为基础的交互作用过程。其决策过程包括五个阶段:情报采集、信息融合、方案设计、决策支持和方案实施,即收集战场态势和装备状况信息,并进行信息融合和统计分析;研究可能的方案,以供决策参考;选择候选方案,并付诸实施;进行实施决策,并收集反馈信息,以用于下一轮决策。因此,系统应能将装备保障的各种因素进行综合和集成,以便能够做出科学、有效的保障方案。

3.1 功能设计

开发装备保障决策支持系统的目的,是为装备保障的管理决策者提供决策支持。因此,系统应具有如下主要功能:① 数据采集与处理功能;② 计算机演示功能;③ 战场态势推演功能;④ 装备保障方案生成功能;⑤ 智能决策功能;⑥ 辅助模拟训练功能;⑦ 远程协作群决策功能。

3.2 平台结构设计

根据装备保障的实际需求,决策支持系统的平台结构如图3所示。

3.3 综合信息处理系统

信息采集与处理是实施辅助决策的先导,由于所需信息类型众多,信息量非常庞大,要求该系统应具有很高的信息处理速度以及可靠性、稳定性和准确性。在多目标、多主体的框架之下,将多个不同类型的模拟结构纳入到同一个混合框架之中,综合运用分布式人工智能、知识的模拟表示以及模糊推理等方法,实行交互式混合推理,以保证决策结果和各主体目标系统的协调性和一致性。

3.4 战场态势评估系统

为使评估结果符合战场实际,采用多批次、多时节、多目标信息融合协作生成多种组合态势方案,并根据需求适时进行人工干预,对战场态势提出质疑,并进行交互式修改、检验。这种评估方式能够从全局上判断所形成的军事态势是否符合军事

原则和作战规律，验证其合理性，并可通过协作机制及时进行反馈和协调，从而获得科学、合理、可靠的评估结果。

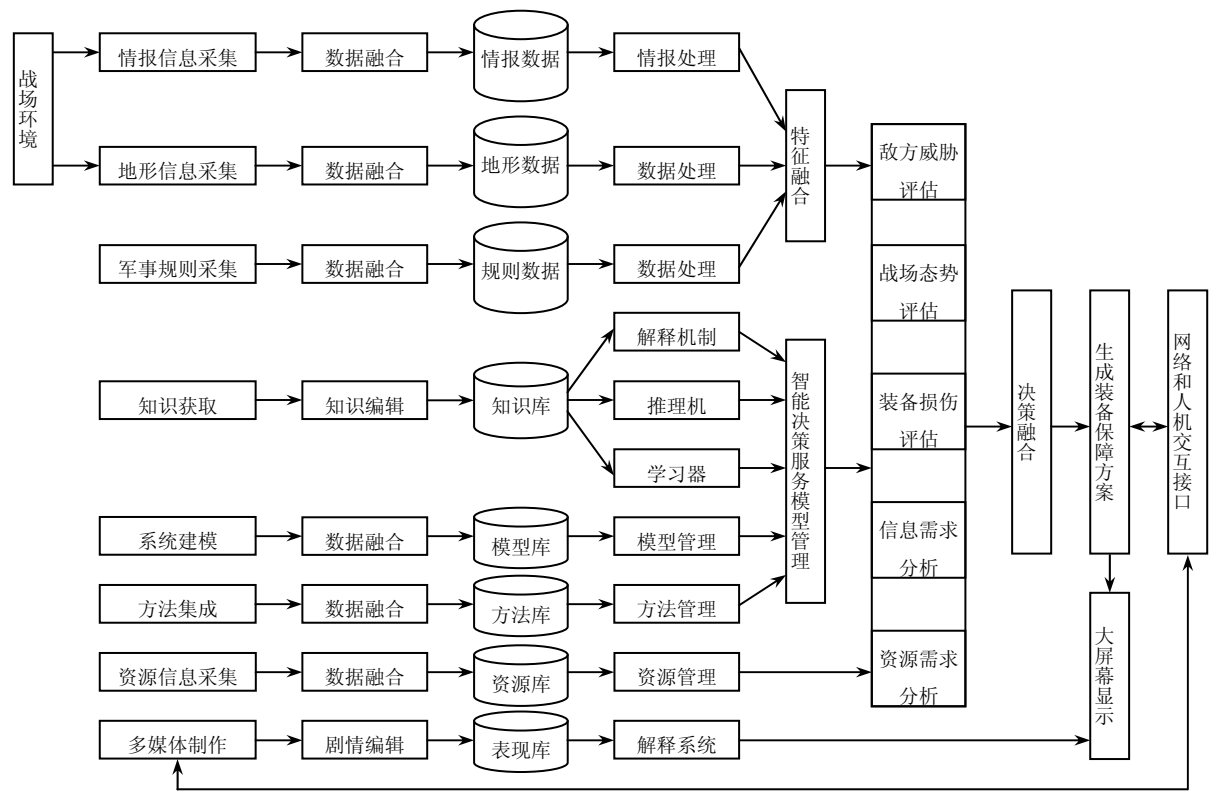


图3 决策支持系统的结构框图

3.5 地理信息系统

地理信息系统是装备保障决策支持系统的重要组成部分，对战场环境的模拟演示起着至关重要的作用，其功能是依据外部地理信息系统所提供的矢

量化的地理信息数据推导出混合推理框架中的战场环境模拟结构及其相应的图模型集，其组成如图4所示。

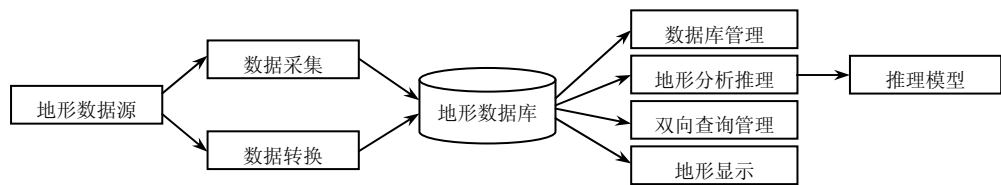


图4 地理信息系统结构

3.6 交互式管理系统

交互式管理系统是决策支持系统的主要部件之一，其功能主要包括数据输入、交互对话、信息显示及结果输出。为使系统具有良好的交互能力，本文采用超媒体技术作为用户界面设计工具，将系统分为前端和后端，前端提供与用户的交互，后端提供计算功能，并将超媒体的基本构件扩展为虚拟确

定、动态计算和过滤。这样，所有的影射和计算都是动态的，并且，超文本引擎独立于决策支持系统，与决策支持系统通过外部消息传递并行运行。

3.7 数据库管理系统

数据库管理系统设计得好坏直接关系到系统的运行效率，由于系统数据类型多，数据量庞大，因此，本文采用了数据仓库（DW）、数据挖掘



(DM)和联机分析技术(OLAP),同时,采用了独立用户视窗技术了管理派生数据,利用 ODBC

技术解决模型库与数据库的集成问题,其结构如图5所示。

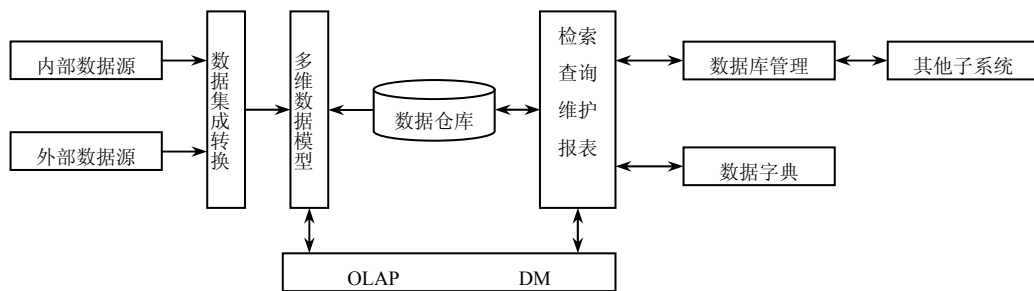


图5 数据库管理系统结构

### 3.8 模型库管理系统

在模型库设计过程中,将目标结构简化为与/或图形,充分体现了目标和资源分配的逻辑依赖关系。同时,采用面向对象的方法来表示简化模型和优化模型,以解决模型与方法、模型与数据的不匹配问题;采用冲突分析、线性规划模型作为问题分析模型;采用多属性效用理论、目标削减作为问题解释模型。为了实现模型重用,本文采用了逆向建模方法,即从现有模型中捕获模型构件。

### 3.9 知识库管理系统

知识库管理系统的主要功能是对控制决策过程中所需的知识进行获取、表示、检索、维护以及检查知识的一致性和完整性,可以帮助用户选择合适的决策模型,完成保障方案的智能分析。该系统包含有用于模型重用和自动生成所需的各种知识,并对决策过程进行推理和解释。本文所设计的系统采用了基于产生式规则和框架的知识表示方法,同时,为使系统不断扩充和完善,采用了基于神经网络的机器学习模式,并将前项推理、逆向推理和模糊推理有机结合,构成了决策的混合推理框架。

此外,系统还包括多媒体制作与表现子系统、保障资源信息管理子系统等,每个子系统都很复杂,限于篇幅,在此不予赘述。

## 4 信息融合与综合决策

由于装备保障决策支持系统是多目标群决策支持系统,因此,含有多个主体结构,所有主体共用相同的战场环境模拟结构BG,而每个主体又有各自的知识数据和评估模拟结构SIT,且SIT是不确

定的,每个图元素都有各自的变化范围,因此,主要采用模糊逻辑来进行推理,并用 Dempster-Shafer 理论进行决策结果的信息融合<sup>[1]</sup>。

### 4.1 基于军事规则的决策模型

设SIT的图模型集为M,  $\forall M \in M$ , 有:

$$M = \langle U, R \cup \{R_i\}, F \cup \{F_j\}, E \cup L \cup \{c_k\}_{k \in K} \rangle \quad (1)$$

其中,  $E \cup L \subseteq U$ ,  $E \cup L$ 中除了有图元素与标签元素外,还有范围性图元素所构成的集合  $Range \subseteq E$ , 通常,  $Range$  为有隶属度函数刻划的动态模糊集合A。设所要识别的候选点集合 $\Omega$ 为A的子集,即:  $\Omega = Supp(A) = \{P | \mu(p) > 0\}$ , 其中P为网格中心点。设  $|\Omega| = n$ , 令:

$N = \sum_{i=1}^n \mu(P_i)$ , 则对任意的  $P_i \in \Omega$ , 可得基本概率分配函数为:

$$m_1(\{P_i\}) = \mu(P_i) / N, i = 1, 2, \dots, n \quad (2)$$

而由  $m_1$  确定的置信度函数  $b_1$  为:  $\forall P_i \in \Omega, b_1(\{P_i\}) = m_1(\{P_i\})$ 。

### 4.2 基于地理信息的决策模型

设按上述方法确定了辨别框 $\Omega$ , 那么, 对每一个中心点属于 $\Omega$ 的网格  $P_i$ , 可通过模糊推理推断出该网格的地形适宜度  $S(P_i)$ , 则由此可得概率分配函数为:

$$m_2(\{P_i\}) = S(P_i) / \sum_{i=1}^n S(P_i) \quad (3)$$

而由  $m_2$  确定的置信度函数  $b_2$  为:  $\forall P_i \in \Omega, b_2(\{P_i\}) = m_2(\{P_i\}), i = 1, 2, \dots, n$ 。

综合考虑军事规则和地理信息, 可根据

Demster-Shafer 理论的融合模型得出融合后的置信度函数  $b_3$  为:

$$b_3(\{P_i\}) = b_1(P_i)b_2(P_i) / 1 - \sum_{j \neq k} b_1(P_j)b_2(P_k) \quad (4)$$

### 4.3 基于情报分析的决策模型

在决策融合过程中, 还应加入情报信息的不确定性, 可用正态模糊隶属函数  $\mu$  来刻画  $P$  点附近这一模糊概念的外延, 以保证在数据融合过程中候选点不会被过早淘汰, 其表达式为:

$$\mu(Q) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(\text{Distance}(P,Q))^2}{2\sigma^2}} \quad (5)$$

其中, 方差  $\sigma$  是一个预先确定的数值, 它反应了在  $P$  点附近这一概念的集中程度。对于  $P_i \in Q$ , 有概率分配函数为:

$$m_3(P_i) = \mu(P_i) / \sum_{j=1}^n \mu(P_j) \quad (6)$$

而对应的置信度为:  $b_3(\{P_i\}) = m_3(\{P_i\}), i=1, 2, \dots, n$

对于其他图元素的推理方法大同小异, 但相对比较复杂, 在此不予一一展开讨论。

### 4.4 决策融合

设决策空间  $\Omega = \{P_1, P_2, \dots, P_n\} = \text{Supp}(A)$ ,  $A$  是可选范围的模糊集, 多主体数为  $i$ , 每个主体  $Agent_k$  的决策向量为  $D_k$ ,  $D_k = (d_{k1}, d_{k2}, \dots, d_{kn})$ ,

其中  $d_{kl}$  为主体  $Agent_k$  给出的置信度。引入反应相关关系密切程度的权重向量  $W = (w_1, w_2, \dots, w_n)$ , 其中,  $w_k \in [0, 1]$ ,  $w_k = 1$  表示完全相关,  $w_k = 0$  表示完全无关, 则我们可以用加权平均来对决策结果进行融合, 即:

$$D = \sum_{k=1}^{i-j} w_k D_k / \sum_{l=1}^{i-j} w_l \quad (7)$$

这一决策融合将整个系统多主体的决策结果进行了更新, 进而消除了决策结果的不一致性。同时, 为了避免自动决策方式下因为强调军事规则而抹杀了有价值的情报信息的情况发生, 可采用人工干预的交互式决策方式, 用户可进一步指示任一  $Agent$  放弃或忽略悖理基例, 也可进行手动更新, 以保证决策结果的正确性、合理性和可靠性。

## 5 结束语

本文针对装备保障的实际需求, 构建了一个信息作战条件下装备保障辅助决策支持系统集成环境, 该系统能够根据作战任务、保障要求、任务类型、力量编成、兵力部属、资源配置、专家知识、历史数据和地理信息等知识, 辅助装备保障指挥人员做出正确的评估与判断, 进而制定出科学、合理的装备保障方案, 对提高装备综合保障能力具有重要意义。

参考文献 (略)

作者联系方式

通信地址: 北京市清河大楼子 8 第二炮兵装备研究院第三研究所

邮政编码: 100085

联系电话: 010-66345310

# VS.NET下信息自动化采集在装备普查中的应用浅析

殷维刚 沈云秋 赵韶平 李霄 赵曦晶

**摘 要:** 装备普查是了解现有武器装备实力的重要途径, 而导弹武器装备体系结构复杂, 信息量大, 不利于普查信息的采集与统计。本文提出了基于.NET 平台的普查信息自动化采集方案, 实现普查信息的快速采集与处理, 这对提高装备管理信息化水平具有一定的意义。

**关键词:** 装备普查; 数据采集; .NET

## 1 引言

装备普查是装备日常管理工作的一项重要内容, 它能够及时反映部队装备实力情况及管理水平。对于导弹武器装备的性能状态和管理现状, 对我军作战与决策具有十分重要的作用。然而, 普查数据的采集绝非易事, 其主要原因是普查涉及到信息的涉及面大, 难以进行统计, 对于导弹武器而言, 每台装备都要进行静态与动态检查, 检查项通常每台装备有数百项, 给数据的统计分析带来了很大的困难。为此, 本文提出一种新的信息采集方案, 在.NET 平台下构建全新的 WORD 自动化数据采集方法, 从 WORD 模板中自动提出相关数据并进行汇总, 达到事半功倍的效果, 该方法在装备普查工作中取得了满意的效果。

## 2 数据自动化采集原理

.NET 平台是微软基于.NET Framework 的一种全新的设计平台, 它较以往开发平台如 VC, VB 等的最大区别在于: 无论采用什么开发语言, 系统均在同一平台下开发与运行, 都是采用 IL (中间语言) 来调用 CLR (公共语言运行时) 进行操作, 并且这些对用户来讲完全是透明的, 用户不用了解其工作原理, 只需应用即可。借鉴功能强大.NET 平台, 采用 Web Service 技术将 Office 应用程序、Windows 应用程序和 Web 应用程序形成一个有机整体, 利用 VS Tools for Office 工具对 WORD 文档进行系统设计, 如表格的输入, 工具条的设置, 按钮事件的响应等, 使之能够实现特定的功能要求, 这就是数据自动化采集原理。这种方法较

VBA 来讲, 具有以下几个优点: 一是.NET 开发功能强大, 利用.NET 框架功能进行设计, .NET 下所有的控件及资源均可以利用, 这将大大提高开发的效率; 二是.NET 安全性高。.NET 采用代码文档分离技术, 所有的代码均编译生成动态链接库文件, 并且所有操作都在 NET Framework 的运行库安全策略的控制下。

这样, 对最终用户而言, 采用 Word 作为数据采集的前端工具, 只是打开 WORD 进行一般的办公操作, 利用 WORD 用熟悉的用户界面和强大的工具, 如例如拼写检查、多语言支持、更改跟踪和数据透视表等, 方便地进行数据录入, 感觉与一般办公操作并无变化, 系统的特殊功能对用户是完全透明的。实际上系统则进行一系列的数据采集操作, 其主要步骤如下。

1) 打开 WORD 应用程序, 利用 Web Service 调用具有托管代码扩展 (指向托管代码程序集的定义属性) 的 Word 文档;

2) 该文档从共享网络位置或文件夹下载编译后的程序集;

3) 该程序集对用户操作所对应的文档工作事件进行响应, 以满足特定的用户需求。利用事件响应函数对需要采集的数据进行数据检验、分析及入库等操作。

## 3 Word 对象模型的应用

在.NET 下提供了多种 Word 对象模型, 开发者只要了解对象模型的使用方法, 就可以有效地对 WORD 数据进行调用。为了更好说明其功能, 下面对几种重要的对象进行介绍。

### 3.1 Application对象

Application 对象是其他 Word 对象的父对象, 提供了大量的控制 Word 的方法和属性。Application 对象的大多数成员应用于全局设置或环境, 而非个别文档的内容。运行 Word 应用程序, 首先要建立 Word 应用对象。Word 应用对象实例名为 ApplicationClass, 只要引用了 Microsoft.Office.Interop.Word 程序集, 就可以使用该对象了。

### 3.2 Document对象

仅仅建立 Word 对象还是不够的, 通常的操作都是具体到某一文档上。在 Word 中处理某个特定文档时, 这个文档就称为活动文档, 并且可通过 Application 对象的 ActiveDocument 属性引用。所有的 Word Document 对象同时也是 Application 对象的 Documents 集合的成员, 该集合由所有打开的文档组成。使用 Document 对象时, 允许使用单个文档, 而 Documents 集合则允许使用所有打开的文档。

### 3.3 Range对象

Range 对象表示文档中的一个连续区域, 通过定义一个起始字符位置和一个结束字符位置可以创建一个范围。您可以在同一文档中同时定义多个 Range 对象, 其使用相互不受影响。当 Range 对象的开始和结束位置定义为同一个字符, 则结果是该范围由一个插入点构成。您也可以将文档的第一个字符作为起始字符, 将其最后一个字符作为结束字符, 从而定义一个包括整个文档的范围。

### 3.4 Bookmark对象

Bookmark 对象与 Range 对象类似, 其使用时通常是先利用 Word 进行定义, 然后通过其名称进行调用。它表示了文档中的连续区域, 既有起

始位置也有结束位置, 可以代表整个文档, 也可以只定义文档中的某一位置。您还可以在文档中定义多个书签, 并且其定义的范围可以重复。

## 4 普查信息采集流程

普查数据采集的方法如下。

1) 设计普查 WORD 模板。根据普查的检查内容要求定制普查所需的表格及检查数据项, 并设定填写数据的大小及位置, 对要录入数据的地方用书签来进行标记, 并配以普查模板填写说明, 以保证数据准确的录入到模板。

2) 定制普查信息采集功能。在.NET 打开前面已设定的 WORD 模板, 添加普查专用工具栏的按钮, 并对响应事件进行设计, 及时对误填数据进行警告, 保证填写的数据的准确无误。

3) 分发普查数据模板。对已设计的 WORD 模板交给检查的单位, 组织进行普查检查, 并按要求进行普查检查项目填写。

4) 汇总已填写的数据模板。对各单位的普查文档, 进行收集, 各单位通过文件夹的形式对 WORD 文档进行管理。

5) 普查信息的采集。利用已开发的系统工具已建好的文件夹进行自动扫描, 逐个文档进行数据采集, 将采集结果存入到数据库中, 以方便统计查询。

6) 普查汇总信息的生成。利用已开发的系统工具从数据库中取出相关数据, 生成有关普查汇总图表和统计数据。

## 5 结束语

Visual Studio .NET 使 Word 自动化技术实现飞跃式发展, 利用.NET 解决方案从 WORD 中提取数据, 实现数据的快速采集工具是一条行之有效的方法。这对于我们研究如何快速采集装备信息, 提高装备管理的信息化水平将起到推动作用。

### 参考文献

[1] <http://www.microsoft.com/china/msdn/library/office/office/OFFmsoffice2003toc.mspx>

### 作者联系方式

通信地址: 北京市清河大楼子 8 二炮装备研究院三所 邮政编码: 100085 联系电话: 010-66345298

# OGSA网络技术在院校信息一体化建设中的应用

由晓民 袁志钢 李艾静

**摘要:** 网格技术是在传统网络技术的基础上发展起来的全新的技术, 该技术最突出的优势就在于将计算、存储、数据、信息等统一作为资源供用户“透明”使用, 极大提升了系统计算能力和整体效能。所有这些特性均是传统的网络技术无法比拟的。为了适应和促进信息化条件下院校教学训练、军事研究和学科建设特别是交叉学科的发展, 本文针对院校信息化建设, 系统地分析了院校信息系统的自身特点、结构和功能, 提出了基于 OGSA 网络技术的院校信息一体化实现方案, 并对关键问题进行了讨论。

**关键词:** 院校信息系统; 信息一体化; 网格技术

## 1 引言

在信息化条件下, 信息的融合与处理对于提高系统整体性和协作性变得尤为重要。就军事院校信息化建设而言, 其中心任务就在于通过对资源的集成一体化, 实现信息高速流动与融合, 为各学科间、各部门间的交流和协作构建起规范、通用和高效的信息平台, 全面提升教学、训练、学科特别是交叉学科的发展水平, 并最终实现院校整体办学水平的飞跃。

资源的集成一体化是现代信息建设的必然趋势和必经阶段, 也是影响和制约院校和学科未来发展的关键问题<sup>[1, 2]</sup>。传统的网络技术虽然解决了计算机和设备间的互连互通问题, 但由于无法对系统资源进行有效管理, 特别是缺乏对信息的分析、处理与融合的有效支持, 造成了大量的“信息孤岛”<sup>[3]</sup>。因此借助传统的网络技术无法在真正意义上实现“资源的集成一体化”这一目标。

而网格技术的出现则为资源的集成一体化提供了必要和可靠的技术支持。该技术最根本的目的就在于将计算、存储、网络、数据、信息、专家、通信等统统作为共享资源, 使得人们能够“透明地”利用这些地域分散的资源完成各种大规模、甚至超大规模的科学计算<sup>[4]</sup>。从这一点可以看出, 网格技术还能有效地减低信息系统的建设成本, 利用廉价的硬件条件实现高复杂度的应用, 其在经济效益方面的优势也是传统网格技术无法比拟的。目前该技术已成功应用于军事仿真领域, 并在信息处理、网络安全等诸多领域显示出巨大的应用潜力<sup>[5, 6]</sup>。

在信息化条件下, 为了更好地适应信息作战、军事协同的要求, 满足前沿学科和交叉学科对信息共享、处理和融合的需求, 本文针对新阶段院校信息化建设问题, 系统地分析了院校信息系统的特点、结构和功能, 并将网格技术应用于院校信息建设, 提出了设计实现方案, 并对关键问题进行了讨论。实现院校信息建设的网格化, 对于院校信息化建设乃至军队训练作战和指挥等活动都有着十分重要的意义和参考价值。

## 2 OGSA网络体系结构

开放网格服务体系结构 OGSA (Open Grid Services Architecture) 是当前最具有代表和影响力的一个开放标准网格的体系结构, 是网格技术实现的重要基础<sup>[6]</sup>。OGSA 是基于网格服务的分布式体系框架, 它以服务为中心, 将计算能力、存储资源、数据资源、信息资源、知识资源、专家资源、通信等资源统一为服务的形式提供给外界使用。OGSA 的体系结构分为五层 (如图 1 所示)。顶层是应用层, 用于运行各学科用户的应用程序; 第二层为汇聚层, 主要负责将服务资源汇聚在一起, 供虚拟组织的应用程序共享、调用, 它主要包括对应用的管理、计划、实施、协调等; 随后是资源层, 包括存储、计算、网络、目录、服务注册、请求等管理协议; 第四层是连接层, 它主要包括与服务器、网络进行连接的实现和连接协议等; 最后一层是构造层, 它包括网络上所有的设备和资源, 如存储系统、计算系统、网络系统、目录、代码仓库等。

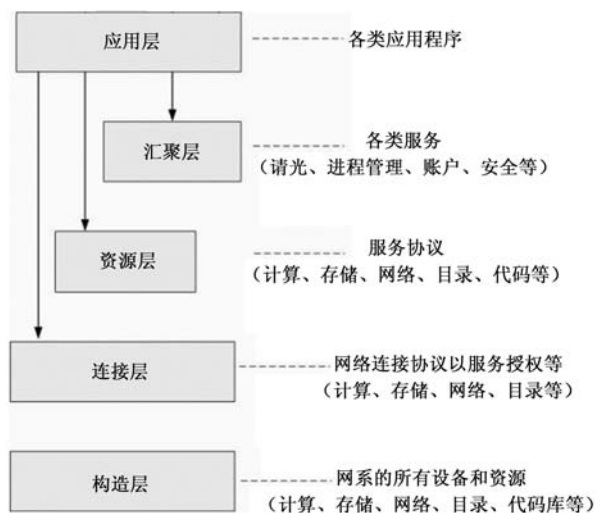


图1 OGSA 体系结构

OGSA 强调服务实例的位置透明性和多协议绑定,支持对底层各种平台设施的集成。在具体实现过程中,OGSA 将 Globus 标准和商业的 Web 服务标准相结合,借助 Web 服务引擎接口中的 XML 消息映射机制有效解决了动态数据的互操作和系统的可扩展性<sup>[6]</sup>。凭借这些特性,OGSA 网络技术在大规模并行计算、大规模高精度军事仿真等领域获得了巨大的成功<sup>[5, 6]</sup>。

### 3 军校信息集成一体化的建设方案

院校教育的信息化是信息技术变革和院校自身发展的必然要求。实现院校的信息一体化建设就是要借助先进网络和信息技术,围绕教学这一中心环节,完成对各种资源的有序化管理和充分共享,充分发挥和提升信息的作用。探索院校信息化建设思路,首先,应做好顶层设计。应在认真研究以往经验教训的基础上,分析当前和未来一段时间院校信息化建设与发展所面临的重难点问题,其次,结合系统特点和中心工作,全面分析信息系统的结构功能,完成好功能的划分工作。再次,对照具体的信息技术体制(这里为 OGSA 网络技术)完成院校信息标准化规范,制订完成网格中各层的具体实施方案。最后,总体部署、统一领导、分步实施。

#### 3.1 现阶段院校信息建设面临的重点问题

1) 专有服务的实现。这里的专有服务是指建立在信息、资源高度共享基础上,针对院校活动特殊需要而实现高级信息服务。现代信息技术的发展

强调信息的高度共享、交叉与融合,也为军队院校的教育、训练、学科发展和军事科研提出了更高的要求。军队院校信息化建设的专有服务则是应对科技发展和军事协同的需要,实现包括高精度大规模军事仿真、规模大计算复杂的学科仿真和依赖于信息融合处理的学科交叉仿真和交叉军事科研,以及专家决策支持系统等在内的高级信息服务。专有服务能最大限度提升院校信息化系统的整体价值,是所有项目中技术含量最高、难度最大的部分,同时也是区别与以往传统网络技术的特色领域。网格技术凭借强大的计算支持能力和天然的信息融合优势,在大规模和超大规模仿真、并行处理和互操作方面有着无可比拟的优势,其在院校信息化建设中必将发挥巨大作用。

2) 高性能的资源共享和管理技术。资源的共享与管理技术主要包括资源的注册、共享、动态分配、回收和使用权限的管理等。该部分内容是信息一体化建设的基础,为院校各功能系统的有序运行及系统间关联提供了必要的支持。由于网格资源存在丰富异构性和多样性,为了确保资源在非协同系统中的“透明”使用和交互,网格中的资源管理技术将变得尤为复杂和细致。

3) 安全机制。具体内容包括系统的安全防盗能力和抗毁能力。网络安全一直是网络建设、特别是军事网络的重中之重。以往的网络技术由于缺乏对全网资源等的一体化管理,其在造成信息闭塞的同时,在安全机制上也存在许多难以应对的问题。与之相比,网格技术则是将全网资源虚拟为一台超级计算机,这种高度有序的管理机制对于在更高水平上应对和解决安全问题有着重要的意义和作用。

4) 信息及协议的标准化问题。院校信息一体化建设本质上实现系统内所有资源的“透明”共享与使用。由于网格资源覆盖面广、种类丰富丰富,如计算能力、存储能力、数据、信息、知识、专家以及通信等,因此信息及协议的标准化问题是网格技术设计实现的关键和基础,主要内容包括基于网格的通用、标准和可扩展的协议与接口、互连互通协议标准、资源管理与交换协议,以及面向专有服务所定义的信息标准和接口等。

#### 3.2 院校信息建设的功能划分

从院校特点角度看,军队院校区别于其他军队单位的最为显著特点是:院校各项工作均是围绕着

教学训练、军事科研工作的顺利进行而具体展开的完备的功能体系，包括教学信息管理、军事训练、军队科研、政治工作、人员管理、财务管理、后勤服务等（如图 2 所示）。在信息化条件下，军队院校信息化建设也必然要围绕“教学-科研”这一中心，以信息一体化为主导，全面深入分析军队院校系统的结构和功能划分，优化信息的管理、共享，推动信息的交叉与融合。院校信息化建设的内容大

体上可以概括为：一个基础平台、一个门户和多个应用系统。一个基础平台借助先进的网络信息技术，特别是网格技术主要解决信息服务多元化和应用系统之间的数据共享和协作问题；一个门户是将应用系统集成起来，为用户提供标准化服务节点；多个应用系统主要解决院校各部门的业务和信息的需求，是院校信息化建设的支撑。

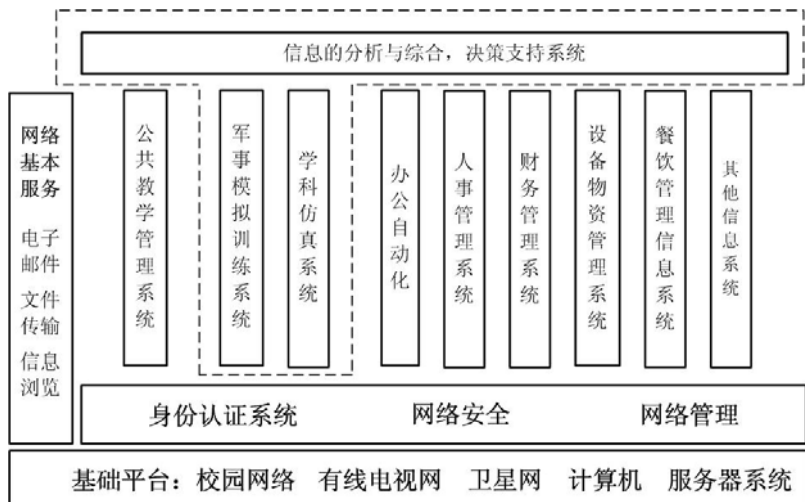


图 2 军队院校信息化建设的结构功能

### 3.3 基于网格技术的院校信息一体化实施方案

的内容可分为以下四个方面，其体系结构如图 3 所示。

参照 OSGA 网络体系模型，院校信息化建设

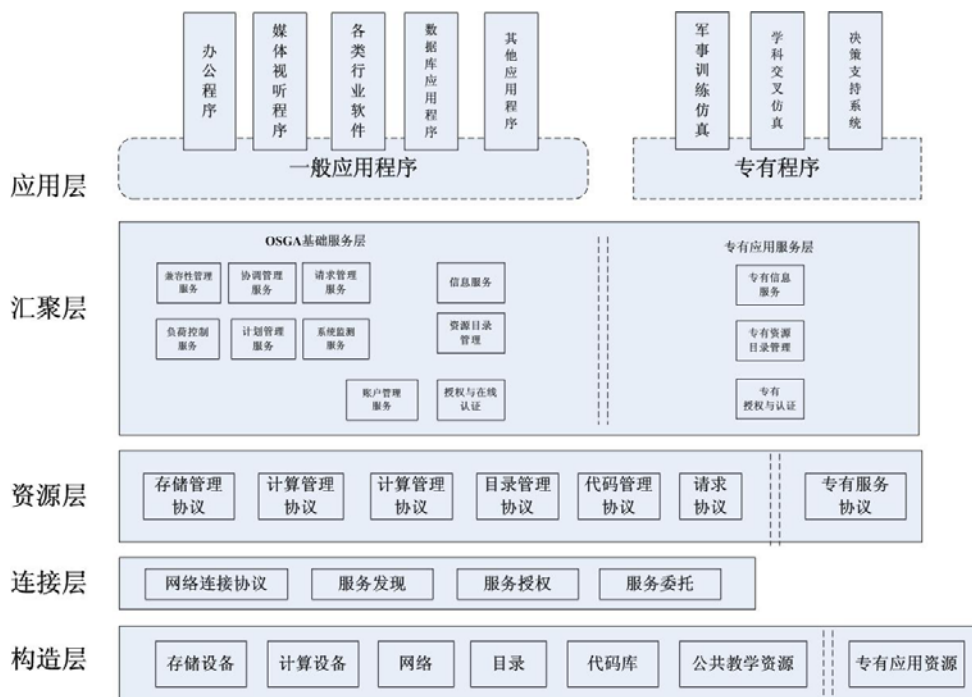


图 3 基于 OSGA 网络的军队院校信息化实现方案

- 基础服务：主要包括院校日常工作和信息的收集，包括办公自动化、教学信息管理、人员信息管理、财务管理、设备和后勤物资管理以及网络连接服务等。
- 共享服务：主要负责完成院校所属的所有资源的共享和使用，包括公共教学资源、计算设备、存储设备、网络设备、科研仪器、各类数据库等。这部分内容由网格技术本身提供。
- 专有服务：主要指借助信息融合与处理实现特殊用途的高级应用，如军事训练仿真、重点学科间的交叉仿真和决策支持等。
- 安全服务：主要包括两方面的内容，即系统的安全防盗能力和抗毁能力。

## 4 结论

在信息技术和协同作战的牵引和推动下，我军院校信息系统建设已开始由传统的实体要素更新转向以信息为核心的系统集成。本文将网格技术与以往传统网络技术相比较，分析研究了采用网格技术实现新阶段院校信息集成一体化建设的必要性和不可替代性。在此基础上，本文将 OGSA 网格技术具体应用于院校信息一体化，系统分析了院校信息系统的结构和功能，提出了院校信息化建设实现方案，并对其关键技术进行了分析探讨。院校信息化建设是军队现代化、信息化的重要内容，并对军队信息化建设起着重要的推动作用。

## 参考文献

- [1] 崔保国,《信息社会的理论与模式》,高等教育出版社,1999。
- [2] 由晓民,“军队院校后勤信息化建设模式研究(硕士论文)”,国防科学技术大学,2004。
- [3] 刘鹏,王立华等著,《走向军事网格时代》(第一章),解放军出版社,2004年。
- [4] 程代伟、何文才、郭荣祥,“新一代网络计算模式分析”,西安科技大学学报,25(2),2005.6。
- [5] 魏洪涛,石峰,李群等,“网格计算在军事仿真中的应用”,系统仿真学报,17(3),2005.5。
- [6] 杨学会,王精业,“OGSA 网格系统及其军事应用探讨”,全国仿真技术学术会议,2005。
- [7] 胡丹露,“地理信息网格及军事应用”,测绘科学,30(1),2005.2。

## 作者联系方式

通信地址:南京市御道街标营2号解放军理工大学通信工程学院

邮政编码:210007

联系电话:025-80828231



# 维修保障交互式电子技术手册（IETM）系统建设研究

张瑞丽 李莉华 王向东

**摘 要：**本文通过现代维修保障对 IETM 的需求，在借鉴美军武器装备 IETM 的基础上，本文对研制第四类型的 IETM 的系统组成、逻辑和物理构架、系统功能、安全要求及需解决的关键技术等进行研究探讨和设想。

**关键词：**维修保障；IETM；建设；研究

## 1 引言

交互式电子技术手册 IETM（Interactive Electronic Technical Manual）自从 20 世纪 90 年代出现以来，已成为美国等许多发达国家所推行的 CALS（持续采办与寿命周期保障）战略的重要组成部分，它不但是装备维修信息化技术研究和应用的热点之一，也是装备维修保障信息化工程的重要组成部分，目前已被成功地应用在多个武器系统的维修保障领域，解决了诸多国家装备使用和维修保障普遍采用纸质技术手册所带来的编制周期长、使用保管不便、重复工作多、耗费大量人力物力财力等诸多问题，大大提高了装备的保障能力和战备能力。依照国际有关标准，按 IETM 的数据格式、显示风格和主要功能方面，可以将其分为 5 个级别：电子索引页面、电子滚动文档、线性结构化 IETM、分层结构化 IETM 和合成数据库 IETM。其中第一类是最简单和最基本的，而第五类是最先进、具有广泛应用前景的电子技术文档，但因为技术原因，还没有推广使用。各类 IETM 各具特点，分别有各自的操作环境和使用要求，目前大多数国家军队使用比较先进的第四类 IETM。另外，随着网络技术的迅猛发展，网络信息资源越来越丰富，基于 WEB 的 IETM 必将渐露头角并将得到广泛应用，这必须将现有的 IETM 实现网络化集成，并建立标准的体系结构。

## 2 维修保障交互式电子技术手册系统开发和应用现状

美国国防部自从 90 年代初提出开展 IETM 项

目的研究与开发以来，经过十多年的努力，已制定了一系列通用规范、标准和手册，用以指导 IETM 的开发、应用与实施，并以统一的格式规范 IETM 的开发质量，使 IETM 能在不同部门之间、不同计算机平台上互操作，进而实现美三军之间的互操作。2003 年美伊战争，IETM 在各类信息化装备中得到充分应用：在“长弓-阿帕奇”（AH-64D）直升机的数字化维修系统中，在“艾布拉姆斯”主战坦克的数字诊断与预测“工具箱”中，都出现了 IETM 的身影，通过 IETM 可以有效提高故障诊断速度，减少维修人员的工作量，改善维修方法和过程。韩国、台湾等其他国家地区军方在美军 IETM 研制技术的基础上，经过研究开发，也形成了适合本国需要的 IETM 技术并在一些装备上进行了应用。

目前，我国军内大部分装备的使用手册、培训手册和维修手册等仍以纸介质为主。随着信息技术的逐步应用，部分装备的电子手册及故障诊断系统相继得到研制开发，有的已交付使用，但是这些系统大都是第三级或第四级的 IETM，而且功能单一、接口封闭、缺乏统一的标准，无法与各类维修手册融为一体，既不能进行智能化的交互，更谈不上网络化的集成。

因此，在我国三军大力推广 IETM 技术，制定相关标准，对 IETM 的数据格式、显示风格做出明确的规定，研制出比较先进的基于数据库管理系统的第四类 IETM，并在设计之初就要考虑到以后容易将其扩展为第五类 IETM 或能与之共存。

## 3 维修保障交互式电子技术手册系统建设研究

在借鉴国内外成熟的 IETM 技术的基础上，根

据现在及未来对武器系统维修保障 IETM 的实际需求，本文拟对将要研制的第四类型的基于数据库管理系统的维修保障 IETM 的软件系统组成、架构、功能、安全要求等方面内容进行方案设计和研究探讨。

3.1 软件系统组成

软件系统由电子技术手册、常见故障维修、维修专家博客、维修技术论坛、网络视频和管理员维护几个系统组成。如下表 1 所示。

表 1 软件系统组成

序号	CSCI 名称	用 途
1	电子技术手册	为用户提供电子技术资料的加载、阅读、更新等功能。
2	常见故障维修	为用户提供常见故障的维修指导。
3	维修专家博客	为维修专家和维修人员提供一个有个人特色的交流平台。
4	维修技术论坛	为维修技术人员提供一个维修技术交流的平台。
5	网络视频	为用户提供即时的视频交互、文件共享和传输功能，以便进行远程故障诊断。
6	管理员维护	可以对系统的重要数据进行维护和管理。

3.2 软件系统构架

3.2.1 软件系统逻辑架构组成

为实现系统功能，在设计时可依据下图 1 所示的逻辑架构进行系统搭建。  
如上图 1 所示，其逻辑架构是基于典型的三层逻辑架构的设计，其系统结构由三个逻辑层组成：

表示层（用户接口层）、逻辑层（服务接口层）、数据层（数据访问层）。该三层逻辑结构的基本思想是把用户界面与处理逻辑分离，由逻辑层来协调客户端与数据库之间的请求，并掌握数据集定义的全部细节和数据库服务器进行通信，这样客户端应用程序就把重点放在显示数据和与用户交互上。

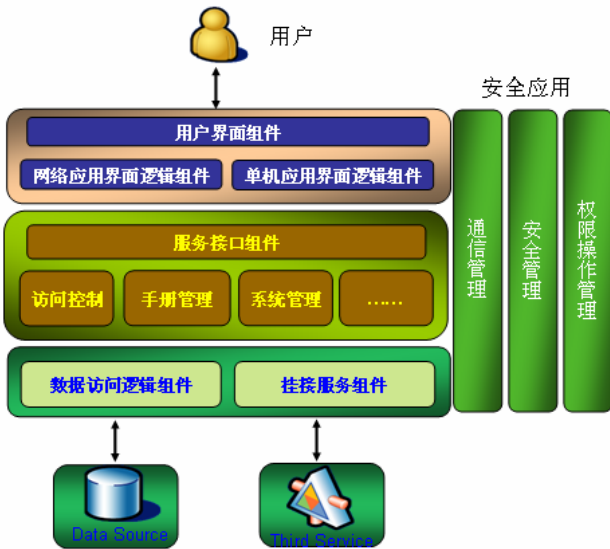


图 1 系统逻辑架构图

3.2.2 软件系统物理应用架构

软件系统的运行环境如下图 2 所示。拟研制的软件系统具有网络版和单机版两个应用系统。其中网络版应用系统可依托于现有的网络环境，系统安

装运行于网络服务器上，系统管理员通过服务器对系统进行管理和维护，授权用户可以通过网络客户端，访问系统内容。单机版应用系统，通过接入局域网也可实现与服务器的数据交换。

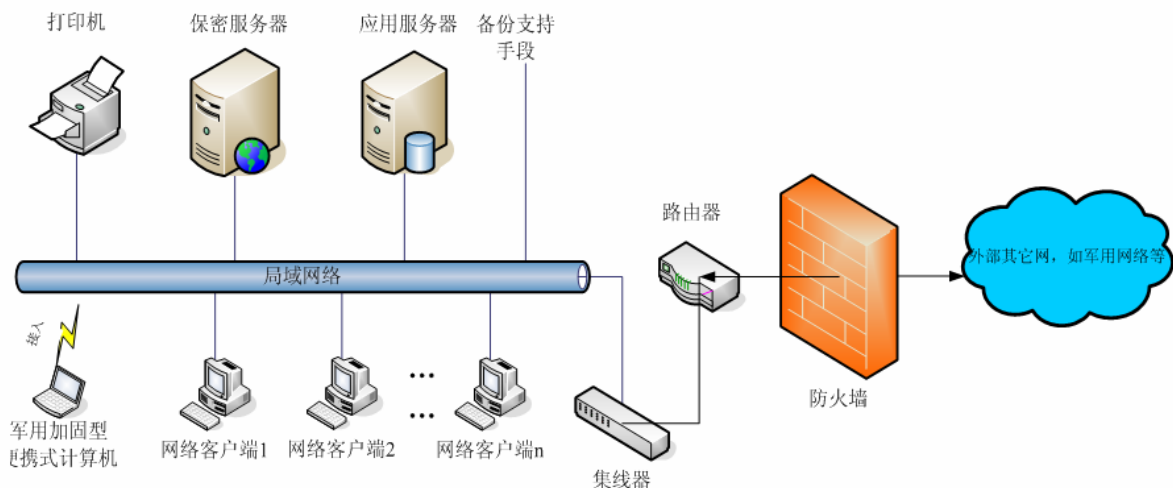


图 2 系统物理架构图

### 3.3 应用系统及其运行的状态和模式

#### 3.3.1 应用系统

考虑到系统的使用环境、运行效率、丰富的应用功能及系统维护能力等方面，维修保障 IETM 应采用 B/S 和 C/S 相结合的应用开发方式完成，具有基于网络和基于单机的两类应用系统。

基于网络连接的 Browser/Server 应用系统是最理想的应用系统。这种系统具有以下特点：分布性好，可以随时随地进行业务处理；功能扩展简单方便，通过修改服务器端即可增加服务器功能；维护简单方便，只需要改变服务器端，即可实现所有用

户的同步更新；必要时通过采用 Ajax（Asynchronous JavaScript and XML）技术可大幅提高页面动态刷新速度，获取较好的交互体验。

基于单机的应用系统的载体是不具备网络连接的设备。本应用系统是一种基于 C/S 开发的应用系统，以便于数据库系统能在无网络的情况下工作（更多的是现场工作），主要实现两部分内容：手册资料的阅读和常见故障的排除。

#### 3.3.2 网络与单机的连接应用模式

网络与单机的连接应用模式共有 3 种，如图 3 所示。

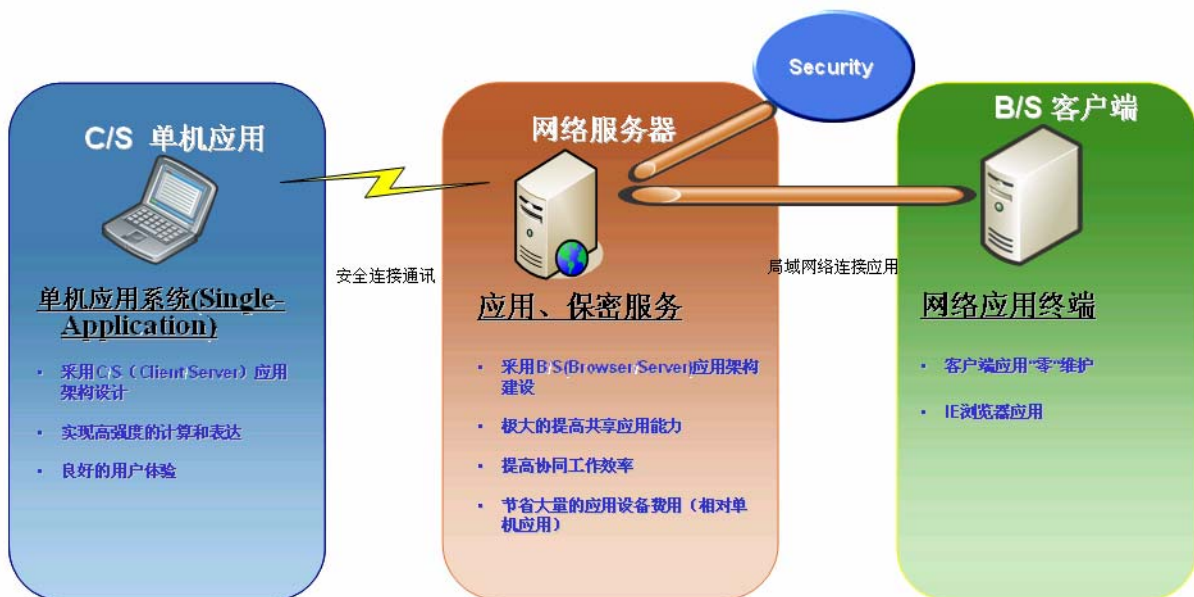


图 3 连接应用模式结构示意图

**与网络连接的应用模式：**此种应用模式是指用户终端设备始终与网络连接（如：军网标准设备终端），此时应用基于网络的应用系统。

**不与网络连接的应用模式：**此种应用模式是指用户单机设备从不与网络连接（如：装备所属设备终端）。此时应用基于单机的应用系统。单机应用系统设备将作为一台独立的设备工作并完成相应的功能。

**与网络偶尔连接的应用模式：**在实际使用过程中，终端设备经常无法保持与网络的稳定连接，只是偶尔与网络进行连接，如在野战维修现场等。很显然，这是经常会遇到的一种状况，这时，必然要求系统的主数据库可以将部分数据复制到终端设备上，形成一个移动数据库。其作业流程为：当单机应用系统的载入设备具备稳定的网络连接时，根据维修任务的需要，单机系统载入设备向主数据库请求下载或同步更新相关的数据库，主数据库答复单机应用系统设备请求，进行数据的下载，从而完成主数据库向单机应用数据库的复制。

### 3.4 软件系统功能

维修保障 IETM 软件系统要着重实现以下功能。

#### 3.4.1 检索功能

提供全文检索功能，能快速检索到系统中的相关信息，根据需要以合适的方式（多种信息表现方式相关结合）展现相关内容。

#### 3.4.2 导航功能

使用者能快速便捷地进入所感兴趣的内容，无需接受培训或通过比较少的培训就能使用该系统。

#### 3.4.3 专家诊断功能

对常见故障或突发故障，能提供一种针对性较强的故障诊断方式，辅助故障定位，提供故障排除方法；能够显示相关故障排除视频或相关的电路图。

#### 3.4.4 远程故障诊断功能

提供远程视频、音频同步传输功能，为远程故障诊断的实施提供安全可靠的支持平台。

#### 3.4.5 互操作性

当具备安全的网络连接时，可在任何一台终端上浏览本系统；同时本系统还可方便地引用其他 IETM 系统或被其他 IETM 系统引用。当一台终端设备出现故障时，通过任何其他一台终端设备即能马上浏览技术信息，无需繁琐的安装及设置过程。

#### 3.4.6 电子讨论区

当用户发现电子技术手册部分中的内容有错误或对手册中的内容持不同意见时，可方便地进入讨论区针对该内容展开讨论。另外，该讨论区还可供用户对使用维修经验进行交流。

#### 3.4.7 维修领域专家BLOG

随着不同的使用时间和使用环境的变化，维修保障人员会对装备维修保障提出新的需求，因此 IETM 系统中的知识也是不断发展的。本系统开设了维修领域专家的专栏 BLOG，由维修领域专家根据实际情况对一些焦点、热点及疑难问题进行系统的讲解，以提高维修保障人员的理论及操作水平，获取最新的维修技能和经验。专栏 BLOG 也提供了一个平台使得维修保障人员可以与领域专家们直接交流。通过这样的平台，既可提高操作号手的专业技能，也可使领域专家及时获知维修保障人员在使用维护中出现的问题并给出解决方案。

#### 3.4.8 自动重编索引及链接

当增加或删除系统中的文件时，系统能够自动重编索引；当越来越多的 IETM 系统被开发出来并链接至本系统时，系统可以自动动态管理链接。

#### 3.4.9 系统管理

包括系统日志、数据备份、用户管理等。本系统可对用户的登录、注销等操作记录加以管理，也可以对各类用户的创建、删除、权限设置等加以管理。

#### 3.4.10 系统的升级和维护

本系统具有良好的开放性，可方便地进行系统的升级和维护。

#### 3.4.11 可扩展性

本系统能够对目前没有，而将来要出现的新的系统功能进行无缝集成和扩充，并为此设计了若干

关键接口，这就使得系统能够灵活适应将来的需要。从某种程度上讲，这一功能使系统能够无限延长自己的使用寿命。

### 3.5 软件系统安全要求

在 IETM 系统中，主要面对的安全风险是用户越权访问和数据在传输时被拦截、窃取和篡改。因此，系统的安全保障设计主要依靠操作系统和数据库自身的安全体系，在系统中划分用户的访问权限和访问级别，在数据传输过程中对所传输的数据进行加密。

#### 3.5.1 充分利用操作系统、数据库自身安全体系

在系统设计过程中，要充分利用操作系统、数据库系统自身的安全特性，不采用任何非常规的方法来实现用户访问授权，避免留下“后门”造成数据被窃取、破坏或篡改。

系统要使用主流、成熟、应用广泛的操作系统版本和数据库，以避免不成熟技术引起的漏洞。对操作系统和数据库要定期进行补丁升级，修补漏洞。在应用系统环境中，使用操作系统的配额机制、数据库的用户标识与鉴别、存取控制、视图、审计和数据加密等安全机制来保障数据的安全和授权访问。

#### 3.5.2 对系统的用户口令进行加密

在系统中，对于数据的保护、业务操作的许可可通过识别用户身份和权限来完成。在传输过程中和数据库中的口令记录字段不能使用明文传递和保存，在口令被传递前对其明文口令最好使用基于 128 位增强型的 3DES 加密算法进行加密，在加密后传输到系统。系统将用户提交的经过加密的口令同数据库中保存的加密口令进行比较，相一致则进行后续操作。通过以上措施和过程，保证了即使加

参考文献（略）

#### 作者联系方式

通信地址：北京市清河大楼子 8 二炮装备研究院第三研究所  
邮政编码：100085

联系电话：010-66345310

密口令被窃取仍不会泄漏原始口令。

## 4 研制维修保障 IETM 系统需解决的关键技术

关键技术之一：实现电子技术手册中目录索引的自动化生成功能，能够自动提取多个 PDF 格式手册文件中的目录信息，组成完整的手册索引目录，便于查阅多部电子手册。

关键技术之二：实现对多个 PDF 格式电子手册文件的跨文件全文检索能力，使得用户可以快速地确定所需信息的位置。

关键技术之三：系统具有可扩展性。它能够对目前没有，而将来要出现的新的系统功能进行无缝集成和扩充，并为此要设计关键的接口，这就使得系统能够灵活适应将来的需要。从某种程度上讲，这一功能使系统能够无限延长自己的使用寿命。

## 5 结束语

维修保障 IETM 系统是我军现代化、信息化和网络化的重要内容，是装备保障过程实现协同操作的必备条件，是提高装备保障水平及武器装备战备完好性的重要手段。计算机技术的飞速发展，使 IETM 的技术、方法和形式多种多样，如果没有共同的开发规范和理论指导，就会导致出现格式各异、互不兼容的 IETM，造成难以维护、共享和互用。因此在 IETM 研制过程中应借鉴美军已有经验和教训，采用当今先进的信息技术和方法，开发我军先进的 IETM，提供各种资源和建立必要的信息标准，研制开发出适应我军武器装备维修保障需求的 IETM 系统。

# 美军新一代战术卫星通信系统—MUOS系统

张献民 虞明宝 刘爱军

**摘 要:** 介绍了美军下一代 UHF 卫星通信系统—MUOS 的发展背景和发展过程; 详细陈述了 MUOS 的关键技术及技术优势; 简述了 MUOS 内部及其与其他系统的互连互通问题; 阐述了 MUOS 发展中面临的挑战, 并针对目前军事卫星通信现状提出了一点建议。

**关键词:** 移动用户目标系统; 特高频后继卫星系统; 卫星通信

## 1 MUOS的发展背景

特高频后继卫星(UHF Follow-on, UFO)系统是当前美军在特高频(Ultra High Frequency, UHF)频段上使用的窄带军事卫星通信(MILSATCOM)系统。该系统具有信号穿透力强、终端实效性好、覆盖范围广等优点, 在近十多年的军事冲突和战争中表现出色, 为各作战单元提供了优良的服务, 得到了广泛的好评。然而, 随着军事需求的发展, 在飞机、潜艇、军舰、坦克、车辆等各军事平台及单兵背负、手持等方式使用的 UHF 终端急剧增多, UFO 系统容量不足的问题日趋明显。一些评估显示 UFO 的用户数量已超过了定额的 150%。但是由于干扰或误操作等原因, 信道可用率通常低于 50%。此外, 目前单兵使用的 UFO 终端还比较大, 携带、使用不是很方便。

移动用户目标系统(Mobile User Objective System, MUOS)是新型窄带军事卫星通信系统。该系统上行频率为 280-322MHz, 下行频率为 338-380MHz, 上下行链路各包含 4 个 5M 带宽的信道<sup>[1]</sup>。系统能够实现全球覆盖, 其通道吞吐量与信息容量远远超出目前使用的 UFO 系统, 可为更多移动用户或固定终端提供窄带语音、传真、低速数据、数字或文字短信、语音邮件等服务<sup>[2]</sup>。未来几年, MUOS 将协助 UFO 系统工作, 并在今后的 20 年内最终替代 UFO 系统。

## 2 MUOS的发展过程

MUOS 的发展计划分为三个阶段实施<sup>[3]</sup>。第一阶段—概念探索阶段, 主要根据 MUOS 的需求研

究系统概念及其体系结构, 全面分析国防部现有通信系统, 研究讨论 MUOS 的商业性能、所用空中媒质、覆盖范围、发展潜能等问题。MUOS 发展的关键是系统过渡、频谱利用率、终端同步、备选策略以及系统的代价、性能、发展进度等问题。经大量研究, 国防部确立了一种更先进的地球同步卫星 UHF 系统为下一代窄带系统的核心。这一阶段为期 21 个月, 已于 2001 年 7 月完成。第二阶段—系统组成部分的进一步研究发展阶段, 主要细化 MUOS 体系结构, 明确外部接口, 分析并解决 MUOS 发展过程中出现的具体技术问题, 借助技术演示、建模、仿真等手段验证系统各组成部分的合理性和关键技术的可行性。这一阶段为期 14 个月, 已于 2004 年 9 月完成。第三阶段—系统发展、演示进而过渡到生产与部署的阶段, 这一阶段现处于关键时期, 正在如火如荼的进行。根据最新预计, MUOS 将于 2010 年发射第一颗卫星同时具备初步的作战能力, 2014 年具备完整的作战能力。

截至 2005 年, 洛克希德-马丁公司(Lockheed Martin)和他的子系统合作者已经成功完成了系统及其子系统的预研论证。在这期间, 政府和合同团队在相关场地进行了系统的研发、集成、模型研制和仿真演示, 并用文档记录了每个合同进度点的系统配置情况。总体来说, 这个团队已经成功完成了系统及所属 13 个子系统的预研论证工作。同时, 政府获准进行主要计划评估, MUOS 发展项目执行办公室与联合战术无线电系统(Joint Tactical Radio System, JTRS)执行办公室、攻防信息系统机构的电信项目办公室、空军改进型一次性运载器(EELV)项目办公室、海军卫星运行中心、国家安全机构、国防合同管理机构都签订了谅解备忘

录。截至 2006 年底,项目发展良好,成本性能指标和进度性能指标都保持在 1.0 以上。目前,项目的主要工作并没有受到影响,发展进度保持着 27 周的提前量。

### 3 MUOS的关键技术及技术优势

MUOS 与 UFO 系统相比,所采用的关键技术有很大不同,具有显著的技术优势,具体体现在以下三个方面。

#### 3.1 卫星星座

MUOS 卫星星座由 4 个地球同步轨道(Geosynchronous Earth Orbit, GEO)卫星和一个在轨备用卫星组成<sup>[4]</sup>,每颗卫星配备一个口径为 12.25 米、包含 16 个波束的可展开天线,从而实现了小型终端在传播损耗严重条件下的可靠通信。MUOS 能在上行链路受到严重干扰、存在闪烁、双层树叶遮挡和有城市多径效应等严酷环境下为舰艇、飞机和地面部队提供更可靠的窄带通信。现今军事冲突多具有区域性特点,借助多波束天线,GEO 卫星可在冲突区域集中使用信道带宽、星上处理、下行功率等,提高使用效能。由于终端不需要跟踪卫星,这样就简化了终端的设计和运行。MUOS 兼容原有的 UHF 终端,能与目前美军使用的 UFO 系统完成协同作战。同时,备用卫星可随时漂移到所需要的地区,以增加这个地区的可用信道数量。

#### 3.2 体系结构

MUOS 基于商用第三代(3G)通用移动通信系统/宽带码分多址(Universal Mobile Telecommunication System/Wideband code division multiple access, UMTS/WCDMA)体系<sup>[5]</sup>。WCDMA 波形采用各自不同的伪随机码扩展基带信号,在接收端解扩,从而允许多个用户使用同一频率,同 UFO 系统相比,其系统容量增加了 10 倍以上,信道可用率大于 97%。MUOS 通过增加链路空闲时间,减少链路阻塞,提高其整体性能。MUOS 可靠语音传输速率高达 9.6kbps,可靠数据传输速率高达 64kbps,最大数据传输速率高达 384kbps<sup>[1]</sup>。

MUOS 内部用户之间信息流的交互方式比以往

的系统有很大改进。MUOS 用户与卫星之间通信采用 WCDMA 上行链路的传输体制,卫星将接收到的信号通过下行馈电链路中继给四个地面站中的一个,这四个地面站分别位于美国的夏威夷(Hawaii)、弗吉尼亚州(Virginia)的诺福克(Norfolk)、意大利的西西里岛(Sicily)及澳大利亚(Australia)。这几个地面站连接着位于夏威夷和弗吉尼亚州的交换和网络管理中心,交换和网管中心识别出信息的目的地,然后通过上行馈电链路将信息发送给卫星,卫星将信息通过 WCDMA 下行链路的传输体制最终转发到目的用户。

UMTS 能提供新的、更高级的业务给用户。UMTS 可以采用上行同步传送计划(Uplink Synchronous Transmission Scheme, USTS)技术<sup>[5]</sup>与全互联网协议中心(all-IP)及互联网协议多媒体子系统(IMS)互连。无线网络已从话音服务发展到多媒体服务,特别是数据服务。IMS 为各种服务和无线接入技术提供服务平台,推动了 all-IP 网的发展。第三代合作伙伴计划(3GPP)使语音网和数据网合并成统一的 IP 网,减少了基础投资。3G 无线网与现存的 IP 网的连接,提供统一的服务平台,使 all-IP 网为无线系统提供 IP 电话、移动 IP 等业务。all-IP 网具备高效的服务质量,数据包传送成功率高达 94.7%。与此同时,all-IP 中心网可为各种业务提供与之相应的服务质量。

#### 3.3 网络管理

MUOS 在网络管理方面优势明显,其由政府控制,具有基于优先权的资源管理能力,可以根据通信业务需求进行调整或做出适当反应。MUOS 卫星的遥测、跟踪和控制(TT&C)由位于加利福尼亚州(California)的海军卫星运行中心(NSOC)来进行,并将空军卫星控制网络(AFSCN)作为备份。这种统一控制、优先处理、备份形式多样、反应迅速的网管理模式必然会在未来的信息化战场体现巨大优势。

### 4 MUOS内部通信及其与其他系统的互连

MUOS 由 MUOS 卫星、MUOS 用户及提供卫星控制、网络控制和网关的地面设备等组成。MUOS 卫星之间通过 60GHz 信号建立链路。



## 5 MUOS面临的挑战

MUOS 遇到的一个问题是经费问题。MUOS 项目已经成功拟定了进度,但能否顺利完成取决于国防部的管理和对将会遇到困难解决。某一个问题的延误了进度,就可能会导致运载工具所拨经费被停止。早些时候,国防部办公厅(OSD)指定海军为 EELV 发射筹集资金并进行招标工作,致使再次估计了整个 MUOS 项目所需经费。前期工作似乎说明,实际运载工具的成本可能要增加,政府正在努力在下次预算中解决这一问题。

MUOS 遇到的另一个问题是信息安全问题。MUOS 系统的安全问题相对于其他的空间项目要明确一些,但是难点在于如何对国家安全局明确的最新安全威胁做出及时响应。虽然 MUOS 项目已经对当前的信息安全问题采取了措施,然而对未来信息安全威胁的不可预知性仍是一个巨大挑战,这必然导致来自技术和经费的压力。

当然, MUOS 发展面临的主要挑战还包括及时确定设计子系统和有效载荷,安排集成工作,解决运载工具的硬件问题等。随着 MUOS 的发展,还会出现许多新的问题。

## 6 结束语

由于 UHF 频段具有其他频段无法比拟的先天优势,其无疑仍是未来战术卫星通信发展的重点。MUOS 借助卫星星座、体系结构及网络管理等关键技术的改进,成功解决了 UFO 系统容量小、速率低、可靠性差等问题,其在未来军事冲突和战争中的作用势必日益突出。考虑到军事卫星通信未来可能面临的战场环境,为争取信息化战争的优势地位,迎接更激烈的军事挑战,必须加快研究和发新一代窄带军事卫星通信系统。

MUOS 支持传统的 DAMA 终端,经新的通用空中接口(Common Air Interface, CAI)实现新型手持终端高效、可靠通信。新的 CAI 应包括一个标准的媒体访问控制(MAC)协议层,以便能够使用现代通信协议,并为语音和无线电通信提供标准化的协议,这些标准化协议能够更容易的扩展 MUOS 网络以外的系统。卫星控制借助国防部管理的 TT & C 分系统来实现。UHF 的按需多址(Demand Assigned Multiple Access, DAMA)控制专线可实现网络控制。MUOS 终端可自动查找控制信道、获取可用服务清单并被动地连接这些服务,从而极大地简化了 UHF 卫星通信的使用。MUOS 与国防信息系统网(Defense Information Systems Network, DISN)、公共开关电话网(PSTN)进行无缝整合可实现互操作性。DISN 由六个子系统组成,即非保密互联网协议路由器网(NIPRNET)、保密互联网协议路由器网(SIPRNET)、国防交换网(DSN)、联合全球情报通信系统(JWICS)、国防保密交换网(DRSN)和视频电视会议系统(VTC)。MUOS 通过 DISN 接口与其他 MILSATCOM 系统互通。传统终端通过 MUOS 网关、DISN 及国有商用网关与移动卫星服务(Mobile Satellite Service, MSS)系统互连,而新型手持终端直接通过 JTRS 与 MSS 系统互连。另外,传统终端与新型手持终端也可经 MUOS 网关直接通信。MUOS 内部通信及其与其他系统互连基本结构如图 1 所示。

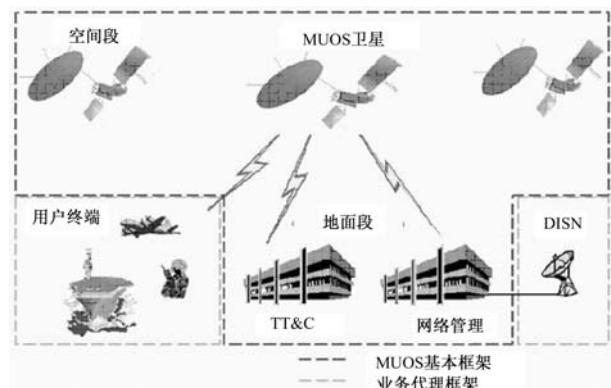


图1 MUOS 内部通信及其与其他系统互连基本框图

参考文献(略)

作者联系方式

通信地址:北京丰台区大成路13号T03

邮政编码:100039

联系电话:010-66820246



# 第三代短波通信网同步管理协议的仿真实现及改进

章锋斌 马大玮 陈正荣

**摘 要:** 本文基于第三代短波通信技术标准, 介绍了同步管理协议的相关概念; 通过采用多线程技术对该协议进行了仿真实现, 证明了其可操作性; 并根据仿真结果对协议做了部分改进, 提高了其可适应性。

**关键词:** 第三代短波通信; 同步管理协议; 多线程仿真

## 1 引言

短波通信具有灵活简洁的技术实现方案、可通达全球的远程通信功能、机动高效的网络组织运用以及特殊环境条件下的通信顽存能力, 被广泛应用于通信、航海、气象等部门, 特别是军事通信领域。

1988年, 美军推出了 MIL-STD-188-141A 系列标准, 即《第二代中高频系统互通性和性能标准》(简称 2G-HF), 为了能够更好地支持大规模数据传输和 Internet 应用, 1999 年的 MIL-STD-188-141B 系列标准(1)和 2001 年的修改版(2)相继诞生, 即《第三代中高频系统互通性和性能标准》(简称 3G-HF)。3G-HF 的改进和优势在于它以同步方式操作, 在高网络负载下有更好的性能。当 3G-HF 网络以同步模式运行时, 其所有的链路建立以及同步数据传输都依赖于站点的同步时钟。3G-HF 网络同步操作通常采用外部方式(如 GPS 接收机)获得时钟, 实现全网同步, 同步管理协议仅起备用补充作用。但当外部参考时间无效或者其他方法行不通时, 3G-HF 网络必须具备同步管理协议的所有功能。

本文主要介绍 3G-HF 同步管理协议及其多线程仿真实现, 并对其做了相应的改进。3G-HF 协议中并没有对该同步管理协议进行测试, 本文的实验数据证明了其可操作性。

## 2 3G-HF同步管理协议

3G-HF 同步管理协议主要包括: 初始时间分配、同步校验握手、同步保持、迟后入网同步四个子协议。它们共同完成以下 3 个任务。

- 1) 对网络内台站时间的初始分配。
- 2) 同步保持, 以补偿时间基准漂移。
- 3) 为迟后入网的站点提供报时服务。

下面介绍该协议中的一些基本概念以及主要同步管理协议数据单元的定义。

### 2.1 驻留组

第三代自动链路建立系统中引入了驻留组的概念, 这种技术将网络中的所有电台划分成多个组。同一时间, 同一驻留组内的电台工作在同一信道上, 而不同的组工作在不同的信道上, 这样可以降低系统的阻塞。在文献 2 中, 一个驻留组在一个信道上的停留时间定义为 5.4 秒, 该时间称为一个驻留时间。

### 2.2 同步数据

为了成功地以同步模式运行, 第三代短波通信系统必须按照网络同步的要求保持时基精确度(50ms 以内)。整个网络的时间定义为存储 GPS 周计数器(0 周是从 1980 年 1 月 6 日 00:00 时开始的), 包括一周中的日、当天经历的秒以及当前秒经历的  $T_{sym}$ 。除了网络时间本地估算外, 每个台站应将时基的误差(精确度的损失)保持在一定限度内。

### 2.3 时间质量

当一个台站将时间更新发送到另一个台站时, 必须按照表 1 对正在发送台站的时基误差进行编码。只有 UTC 部位时间质量可以为 0。来自本地 GPS 接收机, 或误差保持在 1ms 以下的其他稳定时基的台站应报告时间质量 1。一般的台站应使用

最小编码，以确保编码对应的误差大于或等于本地总误差范围。

表 1 3G-ALE 同步管理时间质量码

SM 时间质量码	总的时间误差
0 (000)	无: UTC 台站
1 (001)	1ms: 本地 GPS 接收机或相当于
2 (010)	2ms 或独立的主站
4 (100)	10 ms
5 (101)	20 ms
6 (110)	50 ms
7 (111)	未限制或未知

2.4 同步管理协议数据单元

同步管理协议中用到的协议数据单元（PDU）均为 26bit 格式的数据，其协议结构如图 1 所示。主要包括：呼叫 PDU（LE-Call PDU）、同步校验 PDU（LE-Sync Check PDU）、组时间广播 PDU（LE-GTB PDU）和同步补偿 PDU（LE-Time offset PDU）。

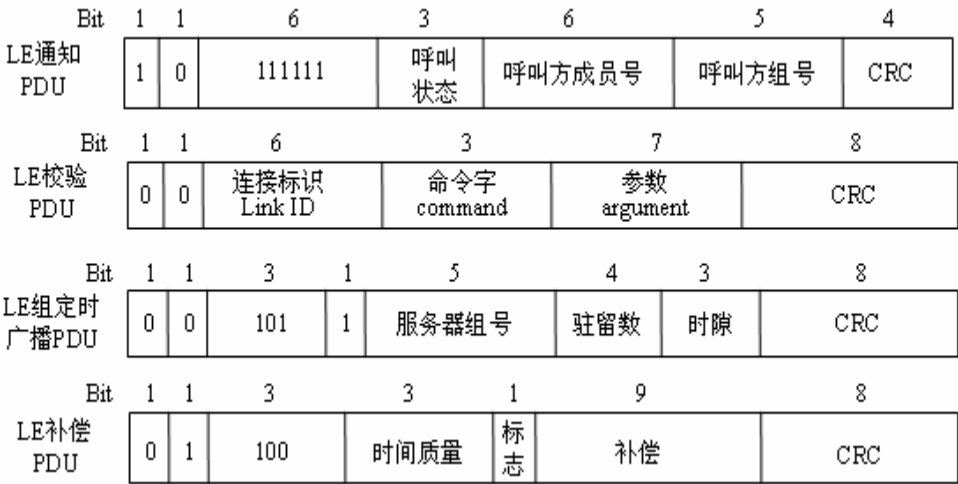


图 1 同步管理 PDU 结构

LE-通知 PDU 是以异步模式发送的，主要用于表明网络的初始时间分配已经开始。LE-GTB PDU 紧跟 LE-通知 PDU 后发送的，主要用于将有限准确度的时间传送到接收它的任何一个台站，完成对各网内各站点的初始时间分配。

LE-Sync Check PDU 和 LE-Time offset PDU 主要用于同步校验握手期间：主叫站点（被校准方）发送 LE-Sync Check PDU，请求时间校验，被叫站点（校准方）回应 LE-Time offset PDU，给出时基漂移和传播延迟；主叫站点接收到 LE-Time offset PDU 后，利用该 PDU 计算其新的本地时间和总的时间误差，再次校准完成网络时钟的同步。

3 同步管理协议的多线程仿真

当 3G-HF 网络运行于同步模式时，为了具备同步管理协议的功能，系统的主要配置包括：主（备用）定时台站、组定时台站和组内各站点成员。主定时台站用于对组定时台站、组内各站点成

员进行初始时间发布，并完成与组定时台站的同步校验握手；组定时台站用于完成对组内各站点成员的同步校验握手；组内站点成员通过与主、组定时台站的时间校准，实现全网站点成员的时钟同步。

为了清晰划分上述三种角色的功能，我们在仿真系统中分别采用三个线程来实现，其多线程仿真实现示意图如图 2 所示。系统启动后，从时刻  $t_0$  到  $t_1$  为第 1 次初始时间发布， $t_1$  到  $t_3$  为网络的第 1 次同步校验握手，系统完成时间同步后，所有的站点在指定的信道上进行同步扫描。在时刻  $t_3$  以后，当站点的时基精确度漂移超过最大误差范围（50ms）时，则主动与主或组定时台站进行同步校验握手。

3.1 主定时台站同步线程

主定时台站不进行同步扫描，只在固定的信道上接收和发送 PDU。其主要功能是在初始启动时进行初始时间分配，完成网络同步后，挂起等待同步校验握手、迟后入网及其他同步请求。

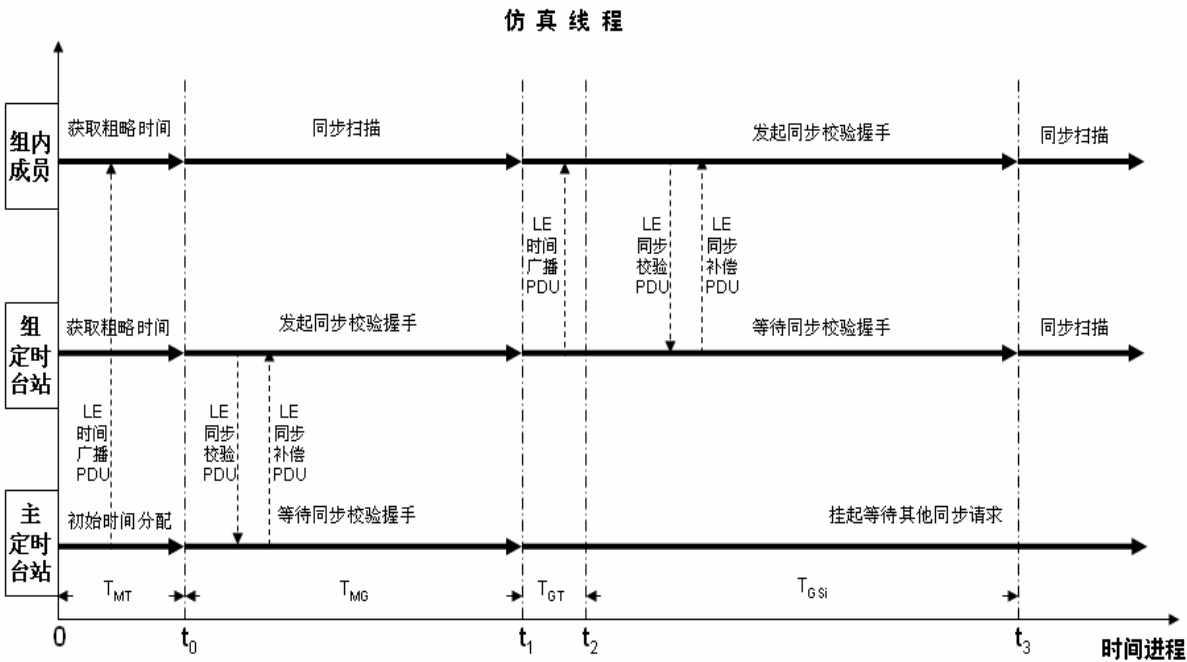


图 2 同步管理多线程仿真示意图

3.2 组定时台站同步线程

组内定时台站的主要功能是在初始时间分配中先与主定时台站进行校准，然后与组内成员进行校准；网络同步后，进行同步扫描，并对同步校验握手请求、迟后入网请求等做出相应操作，同时，不断更新时基以保持本地时钟的同步。

3.3 组内成员同步线程

组内成员同步线程初始处于挂起状态，当接收到主定时台站发来的通知 PDU 后，启动同步线程，获得初始时间并校准；本地同步后，进行同步扫描，同时，不断地更新时基以保持本地时钟的同步。

3.4 协议的中断处理

时间配置协议预期启动后，8 分钟内，未收到来自主定时台站的预期 LE-通知/LE-GTB 序列的任何一驻留组定时台站应启动迟后入网同步协议，呼叫主定时台站；然而，若在所有信道呼叫之后，仍未收到响应，则呼叫指定备用定时台站及其他组定时台站。

4 对同步管理协议的改进

文献 2 中规定：当系统工作于同步模式时，台站地址采用 11 个 bit（低 5 位为组地址，高 6 位为站点地址）的地址码，因此，一个饱和的同步网络最大容量为 32 个驻留组，每组有 60 个独立站点。图 2 所示的同步管理协议是针对饱和网络所设计的，本文针对不同类型（饱和与不饱和）的网络，对协议做了相应的改进，以期能够实现该协议的高适应性。

如果网络中站点的个数及分组信息可知（这在实际应用中可以得到），则可以得到如下公式。

主定时台站首次初始时间分配所需时间

$$TMT = 0.61333 \times N_{group}$$

其中， $N_{group}$  为驻留组数。

主定时台站与组定时台站的同步校准时间

$$TMG = N_{group} \times T_{dwell}$$

其中， $T_{dwell}$  为驻留时间。

各个组内部的同步校验时间

$$TGSi = N_{station} \times T_{dwell}$$

其中， $N_{station}$  为每组内站点数目。

整个初始时间分配的总时间

$$T_{总} = TMT + TMG + \max(TGSi) + TGT$$

其中，TGT 为组定时台站初次时间分配所用时间。

站点均匀分配到各驻留组，不考虑网络延时，信息速率为 2400bps，改进前后完成时间同步所需时间对照表如表 2 所示。

以站点数分别为 96、960 和 1920 为例，假定

表 2 同步所需时间对照表（单位：秒）

类型	站点数/驻留组数	T <sub>MT</sub>	T <sub>MG</sub>	T <sub>GT</sub>	T <sub>GSi</sub>	T <sub>总</sub>
饱和	1920/32	19.63	172.80	5.40	324	521.83
不饱和	96/4	2.45	21.6	5.40	86.4	115.85
	960/16	9.81	86.40	5.40	324	425.61
	960/32	19.63	172.80	5.40	162	359.83
	1920/64	39.25	345.6	5.40	162	552.25
	1920/128	78.5	691.2	5.40	81	856.1

可见，就不饱和网络而言，对于中小型（组数小于 32 个，网内站点数小于 960 个）网络，改进后的协议时间同步完成速度有大幅度度的提高；但对于较大型（组数大于 32 个，网内站点数小于 1920 个）网络，改进后的协议时间同步完成速度则有相应幅度的降低。

况下保证同步网络运行的关键，主要用于实现全网的初始时间分配、同步校验握手、同步保持以及对迟后入网站点的处理。本文通过多线程仿真，对它的可操作性进行了验证，为 3G-HF 同步网络的可靠运行奠定了基础；同时，对协议做的相关改进有利于提高该协议的高适应性。

5 结束语

同步管理协议是在无法获得外部时间基准的情

参考文献

[1] US Department of Defense. Interoperability and performance standards for medium and high frequency radio systems.MIL-STD-188-141B, 1999.

[2] US Department of Defense. MIL-STD-188-141B Notice of Change, 2001.

[3] Kee-Young Shin, Kang Yong Lee, and Kwangyong Lee. CRIT: A Hierarchical Chained-Ripple Time Synchronization in Wireless Sensor Networks. 2006, IEEE.

作者联系方式

通信地址：重庆通信学院通信指挥系

邮政编码：400035

联系方式：13228689768

# 网络数据存储技术及对大型综合数据库建设的启示

赵凡 叶锡庆 徐润平 江帆

**摘 要:** 本论文介绍了网络数据存储技术的发展背景、当前流行的主要网络存储技术,分析了目前大型数据库的数据存储体系结构以及存在的主要问题,提出了建立基于网络存储技术、面向服务的数据中心的建设构想。

**关键词:** 网络数据; 存储技术; 现状; 面向服务

## 1 网络数据存储技术研究

### 1.1 网络数据存储技术的发展背景

数据存储方式采用传统的存储模式称为 DAS (Direct Attached Storage)。在 DAS 存储模式中,存储设备与服务器直接相连<sup>[1]</sup>。服务器的操作系统通常是 Windows、UNIX,即通用操作系统,通用操作系统由多行代码组成,软件非常复杂、庞大,且需要大量昂贵的硬件。配置 Windows、UNIX 的计算机对于执行如网络流量路由、数据库等这样的单独任务并不是理想的选择。随着网络技术的发展,在引发了“设备革命”中,路由器计算机“Cisco”是典型的网络设备代表。“Cisco”由特有的处理器和操作系统软件组成,它只完成一件事情,即引导网络流量。因此能高效地执行路由,并且比通用计算机更便宜、更容易使用。同理,称为“网络文件服务器”的设备,也是网络存储设备,它的操作系统只存储、管理各类数据,因而速度更快、使用更容易。

一个包含几十个节点的大型、巨型信息处理系统中,DAS 存储模式使得数据存储于多服务器中,数据处于非常分散的存储状态。从技术角度看,主要问题一是数据共享性差,难以实现跨平台数据共享;二是即使在局部网络环境下,客户端访问数据必须经过服务器转发,额外开销大,运行效率低;三是可扩展性差,用户存储要求发生变化时,容量难以动态扩展;四是并行性差,对数据库的操作如数据系统备份,会影响到服务器的正常业务;五是安全性差,除了数据的安全完全依赖服务器系统(包括操作系统)的安全性外,在数据分散存储的状态下进行集中备份和异地容灾非常困难。

目前在信息处理系统中广泛采用的 DAS 存储模式,体系结构如图 1 所示。

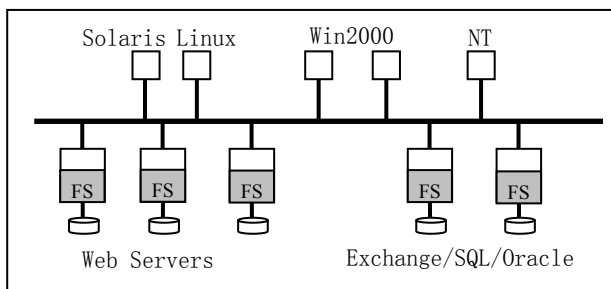


图 1 DAS 的基本架构示意图

其中,阴影部分为服务器的文件系统,即通用操作系统如 Windows、UNIX 等,以及通用的数据库管理系统如 ORACLE 等,协同完成用户的各类请求响应和数据库各种操作。

这种数据存储模式称为以服务器为核心的存储模式。

### 1.2 当前流行的主要网络存储技术

DAS 存储模式已不能满足大型信息系统对数据的存储要求,网络存储应运而生。网络存储是将最新发展的网络技术与存储技术有机结合,将资料分散存储架构转变为信息集中管理的新架构,即网络化架构<sup>[1]</sup>。相对以服务器为核心的存储模式 DAS,网络存储是以数据为核心的存储模式,“网络文件服务器”独立于通用服务器,是网络中的专用计算机设备,它除了配置具专有操作系统外,专配置多磁盘冗余阵列 RAID (Redundant Array of Inexpensive Disks),实现系统的高可用性以及超大存储容量、大数据传输。网络存储是彻底解决当前传统存储方案弱点的有效方案。目前在国际存储设备市场上,各类网络存储设备竞争非常激烈。核心

是实现由数据分散存储为中心转变为网络集中存储为中心。在使用性能方面，网络存储器有自身的操作系统，系统可靠，运作效率高，使用简便，只要透过 IP 网络就可将各种资料（包括数据库和邮件资料等）实现集中化管理，提供实时性的跨平台文件共享环境。传统的应用服务器只扮演单纯应用服务器的角色，其 CPU 可以全速执行应用程序，不用再背负数据访问对磁盘 I/O 的负担。从用户角度看，使用网络存储设备就像使用家电一样，具有更可靠、高效、简便的特性。

当前常见的网络存储技术主要有基于 IP 的网络附加存储 NAS（Network Attached Storage）、存储区域网络 SAN（Storage Area Network）以及 iSCSI 等。

1.2.1 NAS数据存储技术

NAS（网络附加存储）的存储设备是单独的网络设备，从传统服务器上分离出来，直接连接网络进行传输[1]，可为用户提供海量存储和跨平台的文件共享服务。与传统的 DAS 存储模式相比，其优势一是存储系统与客户端直接连接，减少了主机的干预，具有良好可扩展性；二是支持各种主流操作系统平台对各类数据的存储与调用，实现跨平台数据文件共享（可以是异质、异构数据）；三是数据集中存储，减少了系统管理的开销，确保了可靠的数据访问和高可用性；四是基于成熟的以太网技术，容易部署和使用。但网络带宽可能成为瓶颈。NAS 的体系结构如图 2 所示。

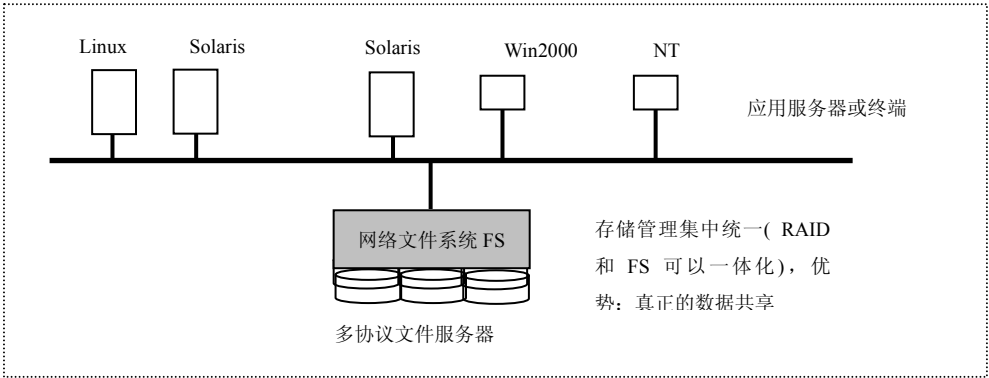


图 2 NAS 的基本架构示意图

1.2.2 SAN存储技术

SAN（存储区域网络）是一个与骨干网分离的独立网络，是在计算机和存储元素之间，以及存储元素和存储元素之间传输数据的专用网络。其基本概念是建立一个存储设备专用的高速光纤通道网络，将所有的存储设备作集中化管理，应用服务器可以访问网络上的任何存储设备[1]。这样，系统具有很强的可扩充能力，数据的访问、备份、恢复不会对网络性能产生影响，同时可提高与远程设备的无缝连接和灾备能力。但主要问题是虽然实现了数据的集中存储，但并不是统一的存储管理，因此数据不能共享；而且主服务器、交换机和存储系统之间的互操作性差；网络管理员必须同时管理和维护两种不同的网络平台。

1.2.3 iSCSI存储技术

iSCSI 存储协议定义了 TCP/IP 网络发送、接受数据块级的存储数据的规则和方法。发送端将 SCSI 命令和数据封装到 TCP/IP 包中，通过网络转发，接受端受到 TCP/IP 包之后，还原为 SCSI 命令和数据去执行，执行完后将返回的 SCSI 命令和数据封装到 TCP/IP 包中在通过网络转发到发送端[1]。支持 iSCSI 技术的服务器和存储设备直接连到现有 IP 交换机和路由器上，具有易安装、成本低廉、不受地理限制、良好的互操作性等优点。

采用 NAS、SAN 和 iSCSI 相结合的数据存储方案也多见。如图 3 所示。

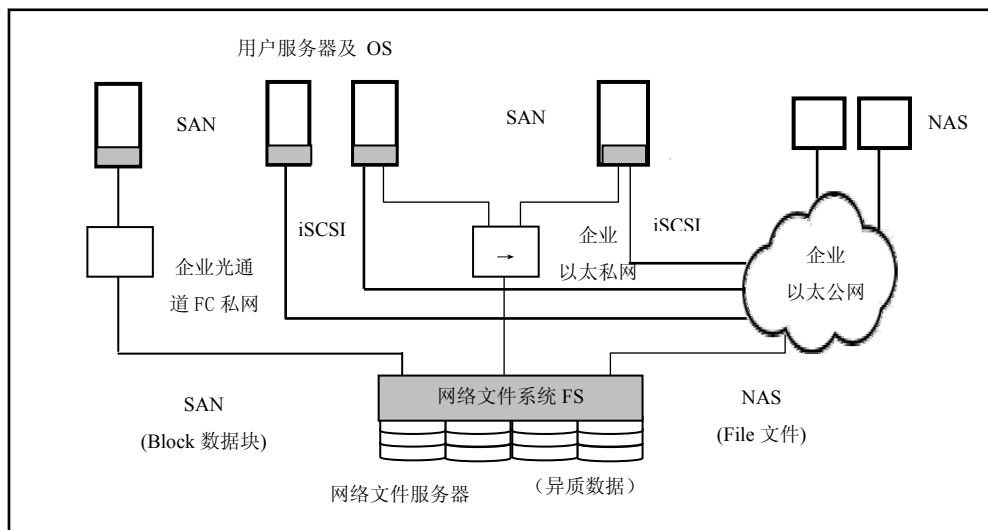


图3 NAS、SAN和iSCSI相结合的数据存储方案

## 2 网络数据存储技术对大型综合数据库建设的启示

### 2.1 采用典型的网络数据存储结构

目前，国内信息处理系统中的数据库体系结构普遍采用 DAS 存储模式。数据库一般嵌入各级各类业务信息处理系统服务器，采用 C/S 结构，客户端通过访问服务器，协同完成各类信息汇集、融合，辅助信息的综合处理与决策。一般小型信息处理系统设置的服务器在肩负数据库的操作的同时，还要对客户端正常业务进行响应处理；大型综合信息处理系统配置了数据库服务器，以专门完成对数据库的存储与操作。但在这两种情况下，作为数据库服务器仍是传统的、通用的服务器产品，使用的是通用型操作系统。

一般来说，各类业务信息处理系统在纵向是多级逐层展开，数据逐层汇总，因此，各类业务信息处理中心均设置数据库服务器；而大型综合信息处理系统是在各级业务处理信息处理的基础上，在每一级要进行多类业务数据的横向集成，这需要设置综合数据库服务器，满足每级对综合数据的使用要求；为实现各类业务数据的有效传递，还要设置数据订阅/分发服务器。同时，这些需要综合处理、汇集、传输的数据，一般是同质数据，即不能实现 UNIX 文件（文件的协议为 NFS）和 Windows 文件（协议是 CIFS），以及与 Web 文件（协议是 HTTP）的互通与共享。因此，不论是各类业务信

息处理系统以及大型综合信息处理系统中，凡采用这种以服务器为核心的数据存储方式，可以说都是一个效率低下的多服务器系统，不可避免地存在并加剧了 DAS 存储模式的种种弊端。

网络数据存储技术的快速发展，对跨多部门、跨地域广泛分布的大型综合数据库的建设提供了巨大的发展机遇。将目前各信息节点基于以服务器为中心的分散数据存储管理，实现向以数据为中心、依托可靠的网络存储技术的数据集中管理的转变，为建设面向服务的综合数据中心的体系结构，为实现信息高度共享、易于数据的管理与集中容灾备份等提供了技术支持。因此依据“依托网络、资源共享、统一保障”的原则，优化数据存储策略和体系结构，建设面向服务的作战综合数据中心已经势在必行。

建设面向服务的数据中心，其数据存储结构采用网络（IP）数据存储技术，典型数据存储结构可以采用如图 3 所示的 NAS、SAN 和 iSCSI 相结合的数据存储方案。

其中，图 3 中网络存储服务器阴影部分为专用操作系统，响应用户请求，高效完成对不同数据的各种操作。并具有可跨平台（Windows、UNIX 等）实现对各类数据如 ORACLES 表、Windows 文件、Web 文件等共享能力。

### 2.2 建立面向服务的数据中心的建设构想

对于跨多部门、跨地域广泛分布的大型综合数据库，考虑到系统的安全性和负载均衡性，在建立

基于网络存储技术的数据中心的同时，应分别建立异地灾备数据中心、移动式数据中心等。

面向服务的数据中心的基本组成与体系结构见图 4。

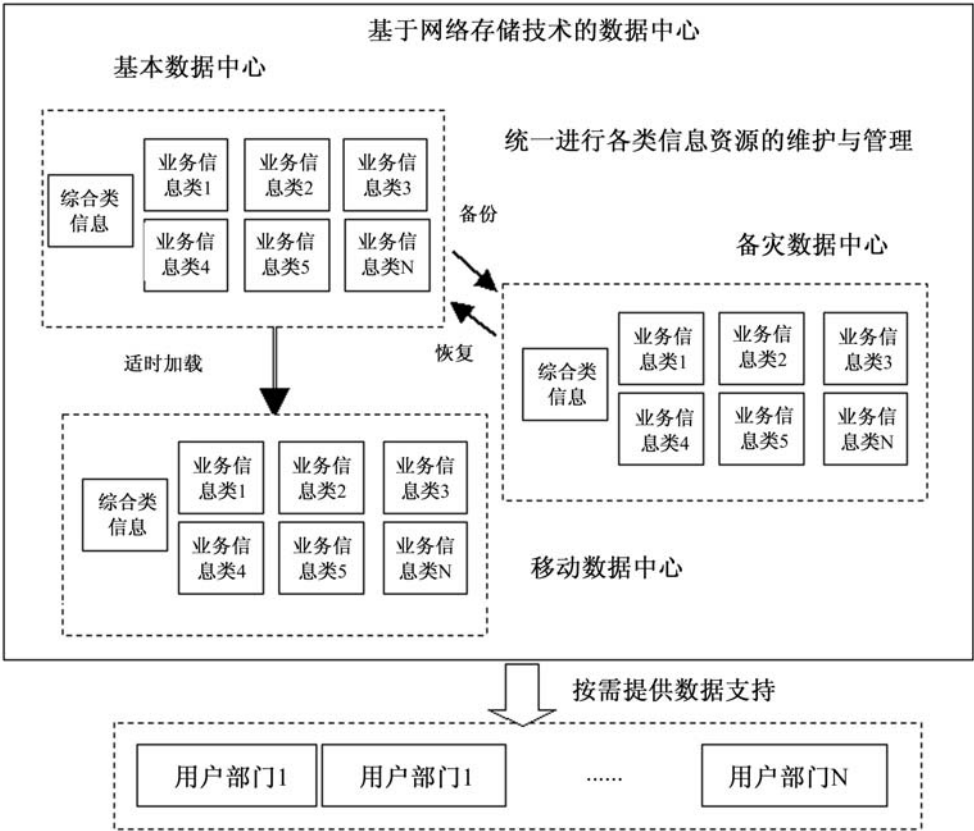


图 4 面向服务的数据中心体系结构示意图

基本数据中心主要功能是统一维护各类数据库信息；定期向移动式数据中心加载更新各类信息；向灾备数据中心实施备灾方案。此外，基本数据中心、移动式数据中心通过计算机网络，按需向各级各类业务信息处理系统以及其他各类用户提供所需数据，并与各类专业信息系统（后台系统）进行数据集成，与上级有关信息处理单元进行信息传输与共享。

这种体系结构的主要优越性，一是减少各级各类信息处理中心数据库的硬件、软件的重复建设，可大大节约硬件、软件经费投资，减少专职维护和管理人员的编制员额，极大地提高各类资源的共享度和利用率；二是便于开展更具专业水准的系统统一管理、维护与升级；三是适应先进的网络存储技术，便于数据的“按需”分发；四是更容易实现数

据系统的集中备份或异地容灾。

当然，在建立面向服务的数据中心的同时，也要建立共享数据资源的管理机制，统一进行共享数据的采集、维护以及使用分发，确保数据中心的各类共享数据全寿命周期的管理；同时要建立数据的技术支持服务机制，确保统一提供对数据使用的技术支持与远程查询服务。

对于军队而言，采用网络数据存储技术和存储结构建设面向服务的数据中心，除上述的可极大减少各级指挥所数据库重复建设的硬件、软件经费投资，便于数据系统的统一管理、护与升级，利于数据的“按需”分发以及更容易实施异地容灾等优越性外，可促进指挥机构信息系统体系结构的转型，使得各级指挥机构建设得更加精练，便于部署和展开。

参考文献（略）

作者联系方式

通信地址：北京市 91566 部队

邮政编码：100036

联系电话：010-66974181



# 基于探索性分析的军事通信网信息优势 评估指标及框架研究

赵新凯 郭晶 孔繁东

**摘 要:** 本文介绍了一种新的系统效能评估方法——探索性分析方法,并将该方法应用于军事通信网信息优势评估分析框架的研究工作,分析了信息优势完备性、准确性指标,利用期望时延概念重新定义时效性指标,提出网系资源利用率指标。提出军事通信网信息优势评估的“两层空间”、“两层体系”和“一层分析”。在此基础上,分析了基于探索性分析方法的效能评估流程,对军事通信网系研究有一定的参考价值。

**关键词:** 探索性分析; 军事通信网; 信息优势; 效能评估

## 1 引言

探索性分析最早来源于美国统计学家 Turkey 1962 年发表的《数据分析的未来》一文,随后于 1977 年出版了《探索性数据分析》一书,引起了统计学界的高度关注。美国 RAND 公司在此基础上,成功开发和应用探索性分析(Exploratory Analysis, EA)方法<sup>[1]</sup>,并在联合一体化应急模型(Joint Integrated Model, JICM)和战略评估系统(Rand Strategy Assessment system, RSAS)的开发中逐步得到完善。该方法应用于多项 RAND 公司的战略分析和评估报告中,如《恐怖的海峡》、《大规模装甲部队入侵的空中打击问题》、《C<sup>4</sup>ISR 对远距离精确打击的影响评估》和《信息时代海军效能评估》等<sup>[2][3][4][5]</sup>。我国国防科技大学管理学院系统仿真实验室开发了 SIM2000 仿真分析环境,其中就运用了探索性分析的基本思想,并引入元建模方法以提高仿真计算的效率。

本文主要针对军事通信网信息优势评估中存在的大量不确定性因素,利用探索性分析方法对不确定性进行研究,并讨论其评估框架建立的问题。

## 2 探索性分析的基本概念

### 2.1 探索性分析的概念和目标

探索性分析目前还没有统一的定义,各学者根据自己研究的课题,给出了不同的看法。国防大学

胡晓峰教授给出了概括性的定义:所谓探索性分析,就是对各种不确定行要素所产生的结果进行的整体性研究。探索性分析的目标是理解不确定性要素对于所研究问题的影响,全面把握各种关键要素;探索可以完成相应任务需求的系统各种能力与策略,进行能力规划,方案寻优,即探索性地得出灵活、高效且适应性强的问题解决方案。

### 2.2 探索性分析的类型

根据探索性分析的不确定性因素可以分为三种探索方式,分别是参数探索、概率探索和混合探索。参数探索的空间主要由各种参数的合理离散值确定的整个或部分不确定性空间;概率探索的不确定性空间是对参数探索不确定性空间的一种补充,它是由分布函数反映的,其输出结果按一定的概率分布。混合探索是指参数探索和概率探索混合的探索。

## 3 信息优势

### 3.1 信息优势的基本概念

应美国国防部的要求,RAND 公司提交了一份探索信息优势的研究报告,分别从物理域、信息域和认知域来度量信息优势,并确定其概念的实现程度<sup>[7]</sup>。

信息优势定义为“不间断的采集、处理和分发信息流,同时阻止敌方完成同样事情的能力”。这

是一种相对的概念，它描述了红蓝双方对战场客观态势感知能力的对比情况。

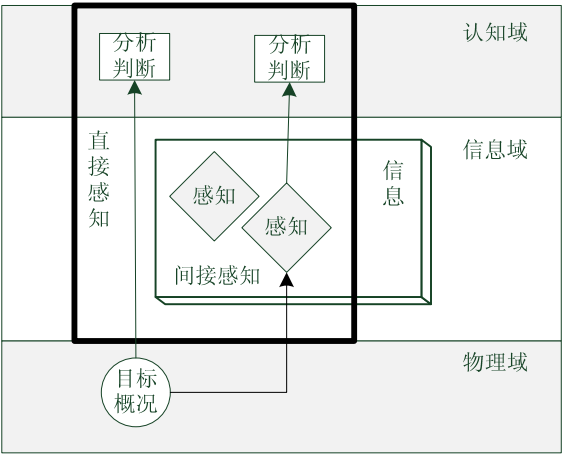


图1 信息优势信息域示意图

3.2 信息优势度量指标

信息优势度量的指标主要分为四种，分别是完备性、准确性、时效性<sup>[8][9]</sup>和网系资源利用率。

3.2.1 完备性

军事通信网信息传输的完备性是指信息经过信息融合处理后，通过网络分发到所有共享态势用户的比例，其完整性主要取决于网络拓扑结构的规划和布置。

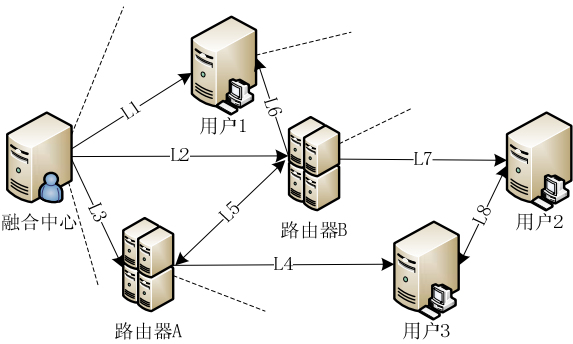


图2 军事通信网拓扑结构图

图2中给出了信息融合中心分别向三个用户分发信息的网络结构图。设第*i*个用户在*t*时刻和融合中心连通的概率为 $P_i(U_i)$ ，则军事通信网信息传输完备性可以用*t*时刻信息融合中心和所有需要向其分发信息的态势信息共享用户的连通概率之积，即如公式(1)所示，*n*为所有用户数，本例中*n*=3。

$$P_t(N) = \prod_{i=1}^n P_i(U_i) \tag{1}$$

3.2.2 正确性

军事通信网信息传输的精确性是指整个通信网向每个用户正确分发态势信息的能力和概率(Probability of Correct Message Recipte, PCMR)。设在*t*时刻信息融合中心*j*正确发送信息的概率为 $P_j(t)$ ，而态势信息共享用户 $U_i$ 从融合中心*j*正确接收信息的概率为 $P_{ij}(t)$ ，整个军事通信网络正确分发态势信息的概率PCMR为所有融合设备到所有用户的联合概率，见公式(2)。

$$PCMR = \prod_{j=1}^m \prod_{i=1}^n P_j(t) \square P_{ij}(t) \tag{2}$$

3.2.3 信息传输的时效性

军事通信网时效性 $\rho$ 可用态势信息从融合中心到用户的“端到端”平均传输时延与期望时延 $\phi(t)$ 之比来衡量。

设信息融合中心向用户发送信息需要经过*w*个网络节点，用户终端移动到指定作战区域所需的时间为*t<sub>m</sub>*，则该路径上的时延总和为

$$T_w = \sum_{i=1}^w T_i + t_m \tag{3}$$

军事通信网有其自身的特点，如网络协作性和通信单元的随机移动性，下面我们将分别讨论各种情况对网络时延所产生的影响，以及时效性的确定。

期望时延 $\phi(t)$ 表示某时刻对通信网络时延的容许程度，此处认为期望时延是信息传输前已经给定，作为已知函数处理。

根据时效性定义，可知

$$\rho = \frac{\phi(t)}{T_w} = \frac{\phi(t)}{\sum_{i=1}^w T_i + t_m} \tag{4}$$

当 $0 < \rho < 1$ 时，网络时延不符合期望要求；当 $1 \leq \rho < +\infty$ 时，网络时延符合期望要求；当 $\rho = 0$ 时，网络无时效性，时延无穷大，认为网络彻底瘫痪。

3.2.4 网系资源利用率

网系资源是指敌我双方在某段时间内能够处理

信息的能力和信道资源。军事通信网在实际应用中,往往不能利用其所有网络资源,从而造成通信网络资源的大大浪费,不能充分体现其真正的信息能力和信息优势,所以考察信息优势,就必须考察其网系资源利用率。在所有军事通信网中最具代表性的是网络带宽,下面我们将就网络带宽展开分析。

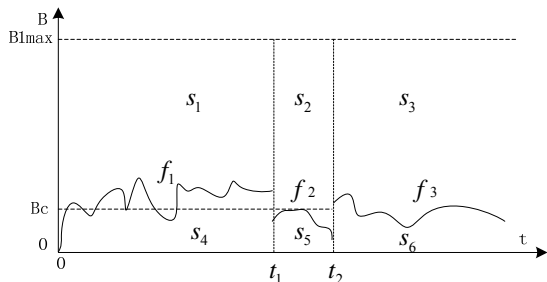


图3 军事通信网系1带宽利用示意图

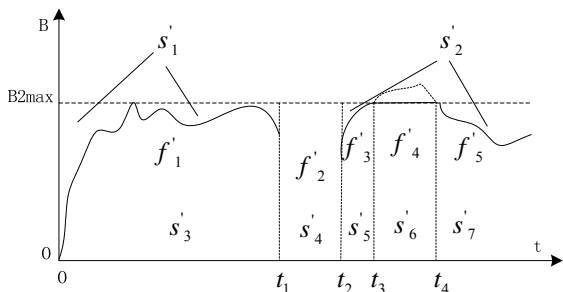


图4 军事通信网系2带宽利用示意图

图3和图4分别给出了军事通信网系1和网系2在某战斗期间过程中的带宽利用情况。其中横轴是时间 $t$ ,纵轴是系统调用的带宽; $B1max$ 、 $B2max$ 和 $Bc$ 分别表示系统1、2的最大可利用带宽和受干扰后系统最大可利用带宽,并有 $B1max > B2max$ ,其中 $t_1$ 到 $t_2$ 时间段内系统均受到敌方的相同程度和方式的干扰, $t_3$ 到 $t_4$ 之间系统2的业务带宽能力不能满足需求。从图中不难发现系统1的信息处理能力要比系统2强,因为系统1的可用带宽要多于系统2(虽然系统1实际使用的要少于系统2),并且在系统受到干扰后,系统1的抗干扰能力要比系统2强。

所以,军事通信网信息能力研究不能局限于已传输信息的完备性、精确性和时效性,也要研究在对抗条件下,网系除了已经使用的资源外,还有多少资源可以供军事信息收集、处理和分发使用,只有这样,才能真正全面地考察军事通信网信息能力。

军事通信网网系资源利用率函数在战争中会被分割成若干个连续函数,设共可以分割为 $n$ 个分段函数,分别表示为 $f_1, f_2, \dots, f_i, \dots, f_n$ , $T$ 为网系资源利用率,则有:

$$T = \frac{\int f dt}{\int B dt} = \frac{\int_0^{t_1} f_1 dt + \int_{t_1}^{t_2} f_2 dt + \dots + \int_{t_{i-1}}^{t_i} f_i dt + \dots + \int_{t_{n-1}}^{t_n} f_n dt}{B \max \cdot t} = \frac{\sum_{i=1}^n \int_{i-1}^i f_i dt}{B \max \cdot t} \quad (5)$$

其中 $B$ 为系统自身能力的一般函数,此处将其自身最大信息能力设为常数 $Bmax$ 。

军事通信网显性信息能力资源指网系在实际应用中所体现出来的信息综合处理能力资源。其对应区域在图3、图4中分别为 $s_4, s_5, s_6$ 及 $s'_3, s'_5, s'_6, s'_7$ 。

军事通信网隐性信息能力资源指网系在应用中除去已经使用的网系能力资源外,所能够继续提供的潜在信息综合处理能力和网系资源。其对应区域在图3、图4中分别为 $s_1, s_2, s_3$ 及 $s'_1, s'_2, s'_4$ 。

根据上述分析可知,军事通信网网系资源利用率 $P$ 也可表示为

$$P = \frac{\text{显性信息能力资源}}{\text{显性信息能力资源} + \text{隐性信息能力资源}} \quad (6)$$

### 3.3 带权重的信息优势

在不同的战役、不同时刻和不同通信任务中,我们对通信网络传输信息的完备性、精确性和时效性的要求是不一样的,所以我们对信息优势进行考察时,赋予三种指标以不同的权重,分别用 $a$ 、 $b$ 和 $c$ 表示。综合上述分析可知,某方在 $i$ 时综合信息能力 $K_i$ 可以表示为

$$K_i = \frac{a \cdot P_i(N) + b \cdot PCMR + c \cdot \rho}{P} \quad (7)$$

其中 $a+b+c=1$ ,当 $a=b=c$ 时,是信息优势的特例,即信息优势完备性、精确性和时效性对军事通信网的权重相同。

从公式(7)不难看出,军事通信网信息能力与网系完整性、精确性和时效性成正比,与时效性网系资源利用率成反比。

则平均信息能力  $K^*$  可以表示为

$$K^* = \frac{1}{k} \sum_{i=1}^k K_i \tag{8}$$

军事通信网相对信息优势可以表示为

$$\Omega^* = \frac{K_R^*}{K_B^*} \tag{9}$$

绝对信息优势可以表示为

$$\Delta^* = K_R^* - K_B^* \tag{10}$$

## 4 探索性军事通信网信息优势效能评估框架

本文所讨论的军事通信网信息优势探索性评估框架可以分为“两层空间”、“两层体系”和“一层分析”共三部分组成<sup>[10][11][12][13]</sup>，其各部分组成关系见图5。

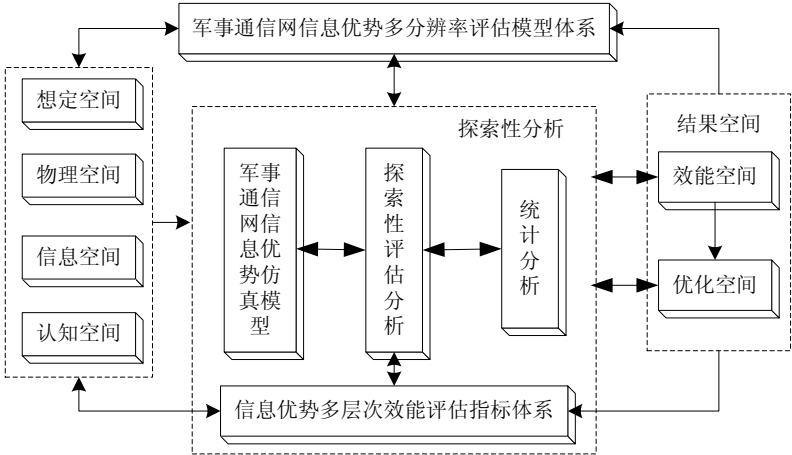


图5 军事通信网信息优势探索性评估框架

### 4.1 “两层空间”

“两层空间”主要由想定参数空间和结果空间组成。想定参数空间包括想定空间、物理空间、信息空间和认知空间；结果空间包括效能空间和优化空间。想定空间包括作战方法和双方任务构想，这是军事通信网实现其信息优势的想定背景。物理空间、信息空间和认知空间分别是信息优势的物理域、信息域和认知域的各种信息等各种参数。效能空间是对信息优势的综合评估，优化空间将根据评估的结果，经过分析后给出系统优化方案。

### 4.2 “两层体系”

“两层体系”包括军事通信网信息优势多层次评估指标体系和信息优势多分辨率评估模型体系。军事通信网信息优势评估指标体系指军事通信网完成我方通信任务，同时压制敌方通信能力的指标参数体系，主要包括完备性、准确性、实效性和网系资源利用率。信息优势评估模型体系提供了想定参数空间到结果空间的映射关系，即建立相关模型，通过探索计算，形成多维可视化图形。建立正确高

效的模型是进行探索性评估的关键，这就需要对信息优势的对象、活动、环境和过程进行全面的考察和分析探索。

### 4.3 “一层分析”

“一层分析”指的是探索性分析，包括效能评估仿真模型、探索性评估分析和统计分析三个步骤。其探索性评估分析包括三个阶段，分别是初步直观探索分析、聚焦探索分析和全面随机仿真探索分析<sup>[5]</sup>。直观探索分析阶段容许所有输入参数以某平均概率发生，探索分析输入参数和综合效能之间的关系。聚焦探索分析阶段探索分析主要集中在发生概率比较高的输入参数范围内。全面随机仿真探索分析不采用已知分布的期望值，而是在任意以此仿真中随机抽取样本进行探索性评估分析。

### 4.4 “流程分析”

首先根据想定参数空间，即想定空间、物理空间、信息空间和认知空间参数，确定信息优势评估模型体系、指标参数体系和仿真模型体系；然后经过探索性仿真，得出结果空间，其中结果空间要给

出系统优化方案，以便军事通信网进一步提高其信息能力，并对评估模型、指标参数模型和仿真模型提出修改意见。

## 5 结束语

通过使用探索性分析方法，考察所有可能空间，很好地分析与综合输入参数和各种想定空间的大量不确定性因素对军事通信网信息优势的影响。

### 参考文献（略）

### 作者联系方式

通信地址：南京市标营2号解放军理工大学通信工程学院

邮政编码：210007

联系电话：010-66820129

在此基础上，通过对探索分析所得结果空间和统计数据的归纳总结，提出对效能评估模型体系、指标体系和仿真模型的优化方案，为下一步效能评估方案提供了优化依据和途径。

探索性分析方法在处理战场大量不确定性因素方面，展现了其特殊的信息处理和分析能力。该方法对于战争需求分析、武器装备效能评估和战场系统优化等课题，具有一定的参考价值。

# 无人作战飞机作战应用问题研究

郑晓辉 刘洪坤

**摘 要:** 文章介绍了无人作战飞机在近几年高技术局部战争中的作战应用情况, 分析了无人作战飞机在作战运用过程中体现出的优势和存在的主要问题, 提出了未来无人作战飞机应用的可能方式和方法。认为未来战争中无人作战飞机主要应用方式和担负的作战任务: 一是有人驾驶飞机与无人作战飞机混合编队作战, 共同执行作战任务; 二是全部使用无人作战飞机编队执行作战任务; 三是使用无人作战飞机参与信息作战任务; 四是使用无人作战飞机执行特殊的作战任务等。

**关键词:** 无人作战飞机; 经验; 教训; 对策

无人作战飞机自越南战争中开始执行战场侦察任务以来, 越来越多地被派上战场。特别是近年来的几场高技术局部战争中, 无人作战飞机更是大显身手, 成为一支不可忽视的重要作战力量。分析无人作战飞机在作战运用过程中体现出的优势和存在的主要问题, 提出了未来可能的应用方式和应用领域, 对于无人作战飞机的研究、开发和应用具有重要意义。

## 1 无人作战飞机在局部战争中的作战应用情况

无人作战飞机自 1917 年诞生后, 并没有很快直接用于战争, 而是等了近半个世纪才作为侦察机走进战场, 又过了 30 多年才直接作为一类作战武器在战场上使用。越南战争期间, 无人作战飞机开始广泛用于执行战场侦察任务。在 1982 年贝卡谷地之战中, 无人作战飞机诱使敌雷达开机, 掩护有人飞机突防, 成功地摧毁了敌人的地空导弹阵地, 其出色表现令世界震惊。在 90 年代以后的四次高技术局部战争中, 凸显了无人作战飞机前所未有的巨大作用。美国及其盟国动用了各自先进的无人作战飞机, 参战的无人作战飞机不仅数量、种类和型号多, 而且能够完成的作战任务也越来越多, 且越来越复杂。在 1999 年的科索沃战争期间, 仅美军的 RQ-1 “捕食者” 无人作战飞机就出动了 3600 多次, 承担了大部分的战场侦察和毁伤评估任务。其机载合成孔径雷达、光电和红外传感器昼夜探测和拍摄各种目标的图像, 并引导北约飞机实施空中打击。在阿富汗战争中, 美军出动携带“海尔法”导

弹的 RQ-1B “捕食者” 无人机, 配合 F-15 战斗机, 成功击毙了本·拉登的助手阿提夫, 首开无人作战飞机对地攻击的先河, 改变了以往无人作战飞机只能执行作战支援任务的角色。在 2003 年的伊拉克战争中, 美军使用了包括“全球鹰”、“影子”、“捕食者”在内的多种型号无人机, 执行战场侦察、通信中继、电子对抗、战损评估、对敌攻击等任务, 为美军提供了“广泛的作战能力”, 任务完成率达 77.2%。另外, 无人作战飞机在伊拉克战争中的表现还论证了美军未来网络中心战的可行性, 甚至导致了新的作战模式的产生。

## 2 无人作战飞机在作战中体现出的优势

### 2.1 便于战场全域配置

无人作战飞机在作战使用中, 一是可根据战场需求采用近、中、远程, 低、中、高空层次性系统配置, 实现战场全域覆盖。二是可根据无人作战飞机主要功能, 进行补充式配置, 实现全频覆盖。如“捕食者”机载“特莎”合成孔径雷达, 活动半径达 3700km, 能够监视 140 万平方公里的区域。三是可采用舰艇、飞机、车载等多种平台搭载, 并根据战场需要, 配置到师、旅、团、营、甚至是连, 使前线部队的活动范围向前延伸 30km, 基本实现了战场全覆盖。

### 2.2 能够执行多种作战任务

现代无人作战飞机种类繁多, 目前已经投入使

用的无人作战飞机多达 75 种。这些无人作战飞机功能各异,除了执行传统的战场侦察监视、通信等任务外,还可用于执行电子对抗、对地攻击等多种任务。在 2003 年的伊拉克战争中,美英两国使用了十多种无人作战飞机,从大型的高空远程“全球鹰”、中高空远程的“捕食者”,到各种尺寸较小、航程较短的小型无人作战飞机,乃至便携式无人作战飞机。遂行的作战任务也从过去单纯的空中侦察,扩展到情报侦察监视、欺骗、干扰、中继、对地攻击等多种作战任务,在战争中发挥了重要作用。

### 2.3 作战使用灵活机动

无人作战飞机一是既可集中使用,以覆盖重要作战地域,又可重点使用,以实现重点目标的全天候饱和侦察监视;二是无人作战飞机不仅可执行作战计划赋予的任务,同时还便于根据无人作战飞机兼容功能进行计划任务以外的作战使用,或者发掘某方面功能进行创造性使用;三是成为整个战场侦察监视系统的一部分,多数无人作战飞机可在高度 10~10000m 的空域自由飞行,便于根据战场情况的变化调整使用。如以色列生产的“云雀”小型无人作战飞机,可在屋顶、窗口或狭窄小巷使用便携式榴弹筒发射,具备多种用途,可实现大区域侦察和重点监控,为作战部队提供实时目标图像,直接支援战斗编队,作战使用非常灵活。

## 3 无人作战飞机作战使用过程中存在的缺陷和问题

纵观无人作战飞机在战场上应用的总体情况,无人作战飞机的战场攻击能力还差强人意,历次战争中主要用于执行侦察、诱饵、空中中继等任务。信息进攻能力不强,硬摧毁能力最弱,空空作战尚未取得战果。总体来看无人作战飞机使用过程中还存在如下一些缺陷和问题。

### 3.1 防护能力弱,战场生存能力不强

无人作战飞机一是速度、飞行高度有限,容易被敌方定位和击落。如“全球鹰”无人作战飞机的飞行速度只有 644 千米/小时,难以逃脱高速战斗机的追杀;尽管它采用了隐身技术,但喷气发动机

工作时仍然会产生一定的红外辐射信号,难免会漏出“尾巴”,一旦被敌方战斗机锁定,将难以逃脱被击落的命运。在科索沃战争中,美军共损失无人作战飞机 27 架,其中 21 架被击落;车臣战争中,俄军也有 3 架“蜜蜂-1”无人作战飞机被击落。二是基于减小载荷考虑,无人作战飞机不像有人驾驶飞机那样拥有多个备份系统,其任何一个关键系统发生故障(如发动机停车、导航控制系统失灵等)都会导致灾难性后果。据统计,目前无人作战飞机的事故率是有人驾驶飞机的 10~100 倍。三是无人作战飞机自动化或智能化程度不高。大部分无人作战飞机只能执行预定任务,中途更改计划的能力十分有限,缺乏应对突发事件和对突然出现的目标做出反应的能力。无人作战飞机的自主飞行控制能力不强,防撞措施不完善,不能做到灵活自动规避目标,其识别真假目标和敌我目标的能力也十分有限。

### 3.2 受复杂气象条件的影响较大

一是作战使用中无人作战飞机结冰问题严重影响其作战使用,在海拔 3050~4270m 的高度上 10~15 分钟就会使飞机受损,冬天和高空环境中问题就更加突出。二是无人作战飞机(特别是小型或微型无人作战飞机)无法在大风天气出动,大大影响了其作战效能的发挥。科索沃战争期间,由于天气的影响,仅美军的“猎人”无人作战飞机就有 15 架提前返回,13 架延期,44 架次作战任务被取消,1 架严重受损。三是无人作战飞机在低云、沙尘和大雾等恶劣的环境、气候条件下,其机载红外摄像机和电视摄像机的侦察效率大大降低,安全回收降落也会受到影响。在第一次车臣战争中,俄军就有 1 架“蜜蜂-1”无人作战飞机在降落时坠毁。

### 3.3 联合作战能力较差

由于无人作战飞机还不能实现与其他无人作战飞机、有人驾驶飞机、地面指挥控制系统的综合集成,因而不具备互连、互通、互操作能力,无法实现信息资源共享。目前,只有美军的“全球鹰”无人作战飞机能与现有的联合部署支援系统(JDISS)和全球指挥控制系统(GCCS)联结,并能将图像直接、实时地传送到相关的用户,而其他类型的无人作战飞机基本上无法实现与现有系统的互连互通。在近年来的几次局部战争中,以美国为

首的多个国家的部队都派出了各自的无人作战飞机参战，但他们的无人作战飞机之间、无人作战飞机与有人作战飞机之间基本上无法协同作战，甚至美军各军兵种之间的无人作战飞机之间进行通信也非常困难，地面控制站经常无法与空中飞行的各种无人作战飞机联络，这对无人作战飞机作战效能的发挥产生很大影响。

### 3.4 操作使用不当，抑制了其作战效能的发挥

由于无人作战飞机是依靠“后方”的地面人员超视距遥控，操纵人员对战场的感知主要是靠卫星提供的视频图像，因而不可避免地会导致操作人员对战场感知能力弱，操作滞后，应变能力差等问题，易被敌方探测系统发现并击落。另一方面，由于无人作战飞机的操控者大多是已经习惯在空中驾驶飞机的飞行员，当他们在面对无人作战飞机进行操控时，其一些在空中的习惯性飞行驾驶意识会给无人作战飞机的飞行带来干扰，难免会造成操作失误。据美军调查，2002 年坠毁的 5 架“捕食者”中，有 2 架就是因为操作人员操作失误造成的。

## 4 无人作战飞机未来作战应用展望

近年来，随着无人作战飞机技术迅速发展，功能不断增强，其作战应用领域不断拓展，使用战术也在不断创新。美国各大司令部 2002 年提交的各战区优先发展的作战能力调查显示，无人作战飞机可完成 117 项军事能力中的 42 项，占总体规划任务的 36%。通过对无人作战飞机发展趋势的研究和作战运用情况的分析，我们认为，无人作战飞机除了执行现有各种作战任务外，未来无人作战飞机运用会出现以下几种方案：

### 4.1 有人驾驶飞机与无人作战飞机混合编队作战

该种运用方式的基本思想是：将各种不同用途的无人作战飞机和有人驾驶飞机组成一个有机的战斗系统。如美军设想在数十千米的空域内，由一架有人战斗机（如 F-22）操控数架无人作战飞机组成一个小机群作战。目前，美国国防部已经在无人作

战飞机的指挥、控制和通信技术，传感器和武器系统技术，以及联合操作软件领域展开了研究。俄罗斯的无人作战飞机发展构想中也提出：将新型的无人作战飞机与第五代战斗机一并组成俄军武器系列，由 1 架有人驾驶飞机通过强大的数据链功能，操作数架无人作战飞机实施空中作战，或支援陆、海军作战。在这种模式中，有人机和无人作战飞机优势互补、分工协作，可以将各自的作战潜力充分发挥。

### 4.2 全无人作战飞机编队

为了提高无人作战飞机的作战效率，拓宽其使用范围，国外近几年提出一种全新的运用概念——无人作战飞机编队。它可以弥补单架无人作战飞机执行任务时面临的问题。无人作战飞机借助其高隐身性和高机动性能，突然出现在作战区域、迅速接近目标，对敌形成合围之势，所以军事专家称之为“狼群”或“群蜂”战术。编队中的无人作战飞机可能是不同类型的无人作战飞机混合编队，也可能是一机多型、系列化的多架无人作战飞机。在若干架外观相同但功能各异的无人作战飞机机群中，可能有诱饵机、侦察机、电子干扰机，还可能混有装备了被动式雷达导引头和战斗部的自杀式无人作战飞机，使敌防空系统防不胜防。

### 4.3 参与信息作战任务

伊拉克战争后，美空军开始研究在电子战、心理战有人驾驶飞机配合下用无人作战飞机实施信息作战的应用模式。旨在通过子母机优势互补，形成辐射源探测与电子干扰、压制一体化的信息对抗模式。在阿富汗战争中，“捕食者”和 AC-130 通过共享传感器和目标信息组成了非常强大的空中打击力量。按照这种运用思路，未来的无人作战飞机还会独立执行更多的信息作战任务，如电子战、心理战、情报战等。

### 4.4 执行特殊作战任务

无人战斗机作为一种全新的武器系统，不但可替代有人战斗机进入生存概率几乎为零的高风险区域执行攻击任务，还可用于执行一些有人飞机尚未承担或无法承担的非常规作战任务。如：抛撒特种物品（投放特种炸弹等）、探测爆炸物、医疗补



给、特种作战支援等。另外，未来的大型无人作战飞机还可用来执行现役空中加油机所担负的任务，其可行性已经得到了论证。

随着无人作战飞机在各种军事活动中的大量、频繁使用，无人作战飞机的使用范围和使用方法也随之扩展。美国陆军战争研究室提出：“军事作战平台要在最需要的区域及时出现，并且能够满足其

军事性能需求。”这表明，未来战争对无人作战飞机的需求是动态的，使用方案在不同的军种中也会有不同的特点。但总的来看，无人作战飞机在未来战争中的运用范围会日益扩大，运用方式更加灵活，运用比例明显增加，作战能力不断增强，并将成为未来战场上可担负多种作战任务的主要武器装备。

### 参考文献

- [1] 杨晶梅.军用无人作战飞机揭秘.北京：国防大学出版社[M].2004.8
- [2] 乙晓光，孙和荣.隐形飞机及其克星.北京：兵器工业出版社[M].2003.10
- [3] 李航航，杨建元.无人作战飞机作战使用与技术发展趋势[J].航空兵器.2003（4）
- [4] 刘洪坤.美国空军转型建设给我们的启示.空军工程大学学报[J].2006（2）
- [5] U.S. DOD. Unmanned Aircraft Systems Roadmap, 2005-2030 2005.8

### 作者联系方式

通信地址：陕西省西安市沣镐路1号176分号

邮政编码：710077

联系电话：029-84799304

# 装备保障信息化软件平台建设

朱敏 高山 徐明 于光辉 黄建建

**摘 要:** 分析国内外装备保障信息化的研究现状,在我军目前装备保障信息化研究理论的基础上,重点阐述保障信息化软件平台建设。介绍了软件平台的相关技术基础,并给出了装备保障信息化软件平台的功能与组成。

**关键词:** 装备保障; 信息化; 软件平台

近年来,世界上发生的几场高技术局部战争表明,除了装备的作战性能之外,装备综合保障能力对战争的胜负具有极其重要的影响。特别是信息化技术在军事领域的广泛应用,引发了一场空前广泛的军事变革,面对这一变革,如何将信息化技术应用到装备综合保障领域,以适应未来战争的需求,在国内外展开了广泛研究。

美军在装备保障信息化方面已经取得了显著的成效<sup>[1]</sup>: ①世界上开发了三军通用的信息系统; ②开发综合武器系统数据库; ③承包商集成技术信息服务; ④交互式电子技术手册。通过以上工作,美军将装备的设计、研制、生产和使用阶段有效集成起来,既保证了装备研制阶段对使用保障阶段的支持,也保证了使用保障经验对装备设计的指导,取得了巨大的军事效益与经济效益,引起了世界各国军事部门的重视。实现装备保障信息的系统集成已经成为世界各国装备保障信息化的重要内容。

国外在装备保障信息化系统建设方面已经比较成熟了,但是我军的装备保障信息化建设中,各军兵种仍处于理论研究阶段<sup>[2-6]</sup>。本文基于这些装备保障信息化理论研究的基础上,重点研究保障信息化软件平台建设。

## 1 软件平台建设相关技术基础

装备保障信息化是一项涉及面广、实施周期长、技术难度高的大型系统工程,需要一整套理论、方法与技术支持。这些理论、方法与技术在不同的层次,从不同的角度帮助人们理解和解决装备保障信息化过程中的各种问题<sup>[7]</sup>。

### 1.1 建模与仿真技术

模型是指为了某个特定目的将研究对象原型所具有的本质属性的某一部分信息经过简化、提炼而构造的表现形式,是对研究对象的一种抽象表示,而非研究对象本身。仿真是在系统建模的基础上,利用数学模型或部分实物对实际的或设想的系统进行动态试验研究。

我军各军兵种装备在全寿命周期的不同阶段装备保障的技术流程与信息流程非常复杂且各有不同,装备保障的技术流程与信息流程建模与仿真是实现全寿命周期多军兵种装备保障信息化软件平台的基础。

装备保障技术流程与信息流程建模与仿真中具有以下特点。

#### (1) 面向任务的建模与仿真

任务建模以对任务或者装备系统的使用想定、使用方案为建模描述对象,以适当的形式表现任务的发生、任务剖面、任务内容、任务时间、任务约束、任务成功条件以及任务执行中突发事件的处理等。对任务的建模水平将直接影响仿真系统与真实使用环境的逼真程度,直至影响到模型的仿真结果。

#### (2) 面向复合型对象系统的建模与仿真

早期的综合保障类仿真模型,通常以一种类型的装备组成的系统为建模研究对象的,而现实中,武器装备的使用部门,通常同时装备着同种装备的多个版本或者完全不同的多种装备,或者更加复杂的情况。因为现代高科技兵器的模块化、通用性不断增强,对一种装备的保障问题必须与同时装备的其他装备的保障问题综合起来考虑,这样才能更加有效地提高保障的质量和费用效能。

### (3) 标准化建模与仿真

随着美国防部 HLA 标准的出台, 仿真模型的开发有了可依据的规范, 也为模型之间的互通、互联、集成以及模型的可重用性奠定了基础。在该标准的基础上, 建立“基于系统的系统”、“基于模型的模型”成为可能, 将作战、训练、使用与维修、综合保障等模型连通在一起, 实现集成化的仿真。

## 1.2 信息集成技术

信息集成的目的是屏蔽底层数据源的异构性, 提供给用户一个统一的视图。

装备保障信息的内容涉及装备生命周期的各个阶段。现阶段我国研制单位和作战部队或多或少开发了一些满足自身需要的信息系统, 这些信息系统是装备保障重要的数据来源。要实现装备保障信息集成, 首先要求新的软件平台能够采集现有信息系统中的装备保障相关信息, 并且新开发的软件平台要能够“即插即用”。这就要求装备保障信息集成平台对操作系统、数据库开发语言和网络等的异构环境具有支持能力, 而且还应具有一定开放性和扩展性。

## 1.3 基于组件和插件的软件开发技术

组件和插件技术将装备保障信息化软件平台通过优化, 分解成合理层次的系列化组件和插件, 并利用这些组件和插件组合成更多更新的通用功能和结构模块。

建立装备保障信息化平台的目的除了实现装备保障信息的共享与集成, 还包括可以方便地在平台基础上, 构建各类装备保障信息系统, 这些信息系统包含各种装备保障应用功能, 例如装备保障能力评估、装备保障方案生成等。采用基于组件和插件的软件开发技术可以在不修改装备保障信息化软件平台的情况下, 可以对软件功能进行扩展与加强, 从而提高了装备保障信息化软件平台的开放性与可扩展性。

## 1.4 装备保障信息化仿真效果评估与优化技术

在装备保障技术流程与信息流程建模与仿真的基础上, 运用多种技术建立的软件平台是否能够满足装备在平时和战时的综合保障需求, 必须通过评估

和优化技术考核仿真效果是否能够满足装备综合保障需要以及满足程度, 并根据考核结果修正、完善软件平台。

## 2 软件平台的功能

软件平台通过系统地研究装备保障信息化平台中的数据集成环境、装备保障信息服务、装备保障模型管理以及装备保障方案评价与优化技术, 实现装备保障信息的数字化、自动化、网络化和集成化, 为全寿命周期的装备保障信息管理、平时和战时的装备保障指挥提供技术手段和决策支持, 从而提高我军装备保障信息化水平。

软件平台主要具有以下三项功能:

- 1) 收集和保存所有不同目的的综合保障信息;
- 2) 完成保障信息化系统过程中所需的分析, 根据可用性和费用对不同的方案进行权衡;
- 3) 完成综合保障信息与其他信息系统的集成。

## 3 软件平台的组成

通过分析软件平台的功能, 将软件平台划分为以下四个可独立运行的组件模块。

- 1) 装备综合保障系统仿真与优化模块;
- 2) 装备综合保障方案模拟与分析模块;
- 3) 装备维修、经验数据积累与分析模块;
- 4) 装备全寿命周期费用分析和优化模块。

### 3.1 装备综合保障系统仿真与优化模块

此模块中, 通过对包括保障站点(库房、补给站、车间等)、装备系统及使用剖面的建模, 建立一个符合工程实际的综合保障优化模型。根据装备系统详细功能分解结构建立维修和保障过程模型。然后将优化配置的备件分配到装备综合保障组织中, 以最大程度地消除综合保障延误时间的影响, 保证最优的可用度指标需求。

此模块中的备件分配优化能力用来对高费用备件进行优化分类和配置, 如对系统可用度和总费用产生重大影响的可修件和不可修件进行优化分类和配置。此模块还可对大量低费用备件的日常供应讲

行概要分析,也可以根据用户需要进行详细分析。

### 3.2 装备综合保障方案模拟与分析模块

此模块是一个功能强大、灵活的计算机仿真软件模型,它主要是用来模拟并分析复杂的装备综合保障方案,支持战备完好性和系统使用保障的相关投资之间的定量权衡。该模型提供与设计输出、综合保障工程、供应链和使用分析相关的接口,能够减少投资风险和费用支出。

此模块与装备综合保障系统仿真与优化模块配合使用时,此模块可以时时提供和系统、备件、资源等相关的信息,同时可以对装备综合保障系统仿真与优化模块解析模型计算出来的配置方案结果进行验证。

### 3.3 装备维修、经验数据积累与分析模块

此模块侧重于分析可靠性随时间发展状况,使用系统结构和定义的费用模型元素来构造和分析与费用流、事件流、费用剖面、趋势预测相关的经验数据。它还提供对授权评估、组件寿命分析和维修间隔期优化的支持。

### 3.4 装备全寿命周期费用分析和优化模块

此模块是进行产品全寿命周期费用分析和优化的有利工具,可用于产品全受命周期费用模型的建立和费用分析。在费用分析的同时考虑产品的寿命时间保障组织特性等,可以针对产品和各级保障站点进行费用计算,其费用敏感性分析结果可以用于费用模型的调整和费用优化。

## 4 结束语

装备保障信息化软件平台是全寿命周期装备保障信息的集成与管理及保障方案评价,为实现装备保障信息化提供技术支持。在全寿命周期的各个阶段、各军兵种、各种部队运用该平台可以对装备保障信息实施管理,在此基础上,可以开发各类装备保障相关应用,包括装备研制阶段的保障性分析,装备使用阶段的保障能力评估,可以辅助保障指挥人员制定平时和战时的装备保障方案。

## 参考文献

- [1] 徐宗昌. 保障性工程[M]. 北京: 兵器工业出版社. 2002
- [2] 孙成立, 刘建军, 徐金强. 对我军装备保障信息化建设的几点思考[J]. 装备保障. 2004 (5)
- [3] 北京军区装备部车船工化部. 对加快通用装备保障信息化建设的思考[J]. 通用装备保障. 2003 (11)
- [4] 王思昌, 冀亚林. 通用装备保障信息化进程中的标准化建设[J]. 军用标准化. 2005 (4)
- [5] 张勇, 吴秀远. 海防部队装备保障信息化建设的几点思考[J]. 通用装备保障. 2005 (3)
- [6] 张瑞丽, 汪荔红. 构建二炮装备综合保障信息平台[J]. 装备. 2002 (3)
- [7] 吴伟仁. 军工制造业数字化[M]. 北京: 原子能出版社. 2005

## 作者联系方式

通信地址: 山东烟台市海军航空工程学院

邮政编码: 264001

联系电话: 13505358526

# 海战场信息资源组织运用方法研究

朱竹青 黄培荣

**摘 要：**随着海军信息化进程的推进，我海战场信息资源规模和质量得到了较大发展，组织运用工作成为发挥和挖掘信息资源作战潜力，提升信息化条件下海上作战效能的重要因素。本文通过分析海战场信息资源组织运用面临的挑战，建立了海战场信息资源组织运用领导体系，提出了“以通信为主导”、“以信息协调为主导”、“以资源优化为主导”和“以远程目标信息精确指示为主导”的海战场信息资源组织运用模式。

**关键词：**信息资源；组织运用；机构设置；运用模式

信息资源是海上作战效能增值的关键因素，组织运用工作则是发挥信息资源整体效能，挖掘信息资源潜在战斗力的重要环节。如何建立精干、高效的海战场信息资源组织运用领导机构，探索海战场信息资源正确的组织运用模式，成为海战场信息化建设急需研究的一项重要课题。

## 1 海战场信息资源组织运用面临的挑战

随着海军信息化进程的不断推进，海战场建设取得了长足进步，但信息资源组织运用还不能完全适应海战场信息化建设的需求。从深层次原因分析，主要面临指挥体制不配套、需求牵引不系统、领导力量不集中、组织运用机制不健全、资源优化能力不强等五个方面的挑战。

### 1.1 指挥体制不配套——信息资源融合性面临挑战

海战场信息资源具有连通性、融合性和可渗透性，要求组织运用工作与指挥体制紧密结合。但是海战场信息资源与当前海军作战指挥体制相对分离的状态，指挥体制不配套，信息资源连通性、融合性和可渗透性面临挑战。

一是以通信为基础的作战指挥体制模式，不利于提供顺畅、便捷的信息交互关系。指挥体制仍然以传统的通信组织指挥手段为基础，没有建立便于海战场信息资源组织运用的指挥机构、指挥关系和职能划分。通信不仅作为指挥的基础支撑，更成为

决定指挥体系的关键，不利于发挥信息资源的连通性、融合性和可渗透性。

二是以功能型为主的作战指挥体制结构，不利于信息流程的组织和信息链路的畅通。以功能为主的指挥体制，追求专业部门门类的齐全，各个专业部门在功能上界线分明。这样的组织结构容易阻断指挥信息流（如树状结构，一环受损，全链皆断），使指挥信息无效地来回流转（如一项工作多个部门来回协调），导致指挥信息链路不畅通，阻碍了横向之间信息沟通。

三是以机械化作战为目的的作战指挥体制运作方法，不利于发挥信息资源的战斗力“倍增效应。”首先，以机械化作战为目的的指挥体制运作方法导致信息资源组织运用脱离作战指挥，作战指挥活动脱离信息资源的组织运用，两者之间不能形成高效的良性互动。其次，海战场信息资源组织运用还不能有效促进指挥机构设置、职能划分和指挥关系的优化。

### 1.2 需求牵引不系统——信息资源系统性面临挑战

需求牵引不仅体现在海战场信息资源的发展建设中，更应体现在信息资源的组织运用中。需求牵引不系统，使得信息资源系统性面临挑战。

由于没有形成基于组织运用需求的海战场信息资源建设需求，装备建设与资源运用容易脱节。在装备建设过程中应将系统的组织运用需求有机纳入需求牵引的范畴，海战场信息资源组织运用需求的内容应当在系统建设中得到很好的体现。美军在信息化发展中，采用的是作战需求→系统需求→技术

需求的发展思路。在作战需求的分析中,要求综合考虑信息资源的建设环境和组织运用环境,全面把握信息资源的作战需求要素和组织运用需求要素,建立基于组织运用的海战场信息资源发展建设需求全面把握信息资源的作战需求要素和组织运用需求要素,建立基于组织运用的海战场信息资源发展建设需求。

尤其应该指出的是,海战场信息资源发展建设需求必须充分考虑组织运用对整个信息资源体系的反馈作用,理清这种反馈作用形成的机理。将组织运用纳入信息资源体系效能评估体系中,强化组织运用对系统建设促进、推动作用。

### 1.3 领导力量不集中——信息资源复杂性面临挑战

海战场信息资源几乎涵盖了能够为海上作战提供信息支撑能力的所有软硬件资源,各职能部门对系统建设权利紧抓不放,对系统组织运用则互相推委、不愿意管、不愿意抓,领导力量不集中正成为海战场信息资源组织运用中面临的重要问题,信息资源复杂性在组织运用工作中面临挑战。一是容易导致海战场信息资源组织性差,整体效能难以发挥。由于没有权威的领导力量对海战场信息资源组织运用工作常抓常管,组织运用工作分散于各个子系统,各分系统之间电磁不兼容、信道挤占、互不连互通、信息泛滥等问题将难以很好解决。二是难以使有限的信息资源组织运用力量形成整体合力,不利于组织运用工作效能的发挥。缺乏集中统一的领导力量,将导致信息资源组织运用力量分散,管理成效不高,限制了对海战场信息资源体系潜在战斗能力的转化和挖掘。

### 1.4 运用机制不健全——组织运用特殊性面临挑战

海战场信息资源组织运用是一项全新的工作,尚处于起步和探索阶段。既缺乏实战中信息资源组织运用经验,也缺乏健全的组织运用机制。具体表现为以下几方面。

一是缺乏整体协作机制。各分系统之间、各业务部门之间没有建立整体协作机制,互不相干、互不关联。

二是缺乏科学、规范、专业化的组织运用程序和方法。对海战场信息资源组织运用的内容、方

法、程序上还缺乏真正深入的研究,没有形成科学、高效、系统、规范的法规、规定。

三是信息资源组织运用力量的发展与组织运用需求不相协调。各级组织运用部(分)队编制人员少、力量单薄、人才来源渠道窄,保障少力量、运用缺支撑的问题普遍存在。

四是缺乏海战场信息资源组织运用效果的评估标准和方法。对信息资源组织运用效果的评价体系还没有形成,对组织运用的实际效果还缺乏有效的评估标准。

五是没有形成系统的组织运用法规体系,规章制度、条令条例还不完善。海战场信息资源如何配置、如何优化组合、转移等一系列问题在法规上还找不到解决的办法。

### 1.5 资源优化能力不强——信息资源配置的灵活性面临挑战

海战场信息资源组织运用中面临组织运用力量有限和组织运用任务繁重的双重考验,资源优化能力不强也成为组织运用工作中需要解决的重要问题,信息资源灵活配置的优势面临挑战。

一是优化配置能力不强。一方面,信息资源要素与指挥节点不能实现有机融合,不能为指挥节点的运作提供最佳的信息支撑能力;另一方面,信息资源要素与海战场信息流程不相适应。海战场信息资源要素不能有效释放信息获取、信息处理和信息传输的信息支撑效能。其三,信息资源要素与其他信息要素之间的协调、配合能力变差。信息资源要素不能有效从其他信息资源要素那里获得支持,同时也不能对其他信息资源要素提供有力的增殖服务;其四,信息资源要素与整个信息资源体系的运作不相协调。单个的信息资源要素不能完全融于信息资源体系的运作,没有形成系统中局部功能对整体功能非线性增殖效应。

二是优化组合能力不强。一方面,信息资源要素种类之间的组合不是最优。没有充分考虑海战场信息资源要素的各自特性,根据功能需要将各要素简单搭配,组合成具有一定功能的子系统;另一方面,不能实现信息资源组合中的精确优化。数量上,不能实现信息资源组合中的定量优化;质量上,不能实现有限的资源要素实现最大的效能组合。其三,信息资源要素组合次序不是最优。信息资源要素在海战场信息流程中都处于相应的工作序

列上,当这种工作序列不利于发挥各要素最大工作效能时,这种工作序列对信息资源要素而言就不是最优的组合次序。

三是动态筹划能力不强。动态筹划就是要求海战场信息资源组织运用中,根据海上作战的实际需要尤其是海战场情况的实际变化,实时决策和实时计划,动态赋予或调整海战场信息资源担负的任务,实现海战场信息资源与作战任务之间的最佳匹配,最大限度地发挥海战场信息资源的作战效能。海战场信息资源组织运用动态筹划能力不强集中体现为信息资源与作战任务之间的固化,信息资源效能发挥对战场情况变化的适应性不强,信息资源组织运用缺乏动态灵活性。

四是信息流程优化能力不强。优化的信息流程就是要求海战场信息资源组织运用中,能够形成顺畅、高效的信息链路,确保信息在指挥节点、职能部门内、外部“进得来、出得去”,进而形成高效的信息“进出、反馈和再生”流程。海战场信息资源组织运用中信息流程的优化能力不强主要表现为信息流程环节繁多、信息无效流动加剧、信息再生质量变低、信息反馈效能低下等。

## 2 海战场信息资源组织运用领导体系

海战场信息资源组织运用领导体系是关于海战场信息资源组织运用领导机构设置、职能划分和相互之间关系确定的基本方法和措施,主要包括领导机构的设置和各级机构职能的划分。

海战场信息资源组织运用领导机构的设置必须立足现有的海军作战指挥体制,平时以司令部为主体、战时以指挥所为主体组织实施。根据信息化条件下海上作战的基本规律,海战场信息资源组织运用领导机构的设置应当分别针对海军平时、参加联合作战和海军独立作战的不同情况,建立与之相适应的职能机构。

### 2.1 平时组织运用领导机构设置

平时海战场信息资源组织运用的管理协调机构,按海军平时组织领导序列设立。各级领导机关常设“信息资源组织运用管理协调中心”;作战部队在其指挥所内分别设立相应的信息资源组织运用管理协调组。

## 2.2 战时组织运用领导机构设置

### 2.2.1 参加联合作战时组织运用领导机构设置

参加联合作战,海战场信息资源组织运用必须与联合作战指挥体制相适应,在联合作战指挥部的统一部署下,强调海战场信息资源的集中使用,同时必须搞好与其他诸军兵种的协调与配合。首先应在“全军信息资源组织运用中心”下,建立“联合作战信息资源统一协调中心”,以统一协调联合作战各军兵种信息资源的组织运用;此外,还需建立“海上作战信息资源组织运用协调中心”,下设“岸基信息资源组织运用协调组”和“海上作战兵力信息资源组织运用协调组”。

### 2.2.2 海军独立作战时组织运用领导机构设置

海军独立作战时,按海军指挥序列设立各级信息资源组织运用协调机构。设立“海战场信息资源组织运用协调中心”,下设“岸基信息资源组织运用协调组”,各参战军兵种设置相应的信息资源组织运用协调组。

## 3 海战场信息资源组织运用模式

针对当前我军组织指挥体制的实际情况,吸收外军关于信息资源组织运用的相关经验,现阶段我海军海战场信息资源可能采取的组织运用模式主要有以通信为主导的组织运用模式、以信息协调为主导的组织运用模式、以资源优化为主导的组织运用模式、以目标信息精确指示为主导的组织运用模式。

### 3.1 以为通信主导的组织运用模式

以通信为主导的组织运用模式,平时以司令部通信部门为主体,在参谋长的领导下,组织筹划海战场信息资源的作战运用工作。战时相应地主要以指挥所通信中心为主体,在参谋长的领导下,拟制组织运用工作计划、指示,组织系统的建立、运行和接替、转移等工作。

这种模式的优点是:战时由通信中心为主体负责海战场信息资源组织运用的具体实施,与平时由司令部通信部门为主体的现行职责一致,利于快速进行平战转换,职责明确,实施难度较低。而其主要缺点是:战时通信中心不掌握作战整体情况,需

要与指挥中心等其他中心做大量的协调工作,可能导致系统难以根据复杂多变的战场情况及时做出反应,对系统效能的发挥会造成一定的影响;平时通信部门虽然负有指挥信息系统建设管理的职责,但就目前的情况看,其职责范围主要限于通信系统,对于涵盖范围更广的海战场信息资源情况的掌握还比较有限。且对平时作战值班、应付突发事件等总体情况难以掌握,同样需要做大量的协调工作,可能会影响整体效能的发挥。

### 3.2 以信息协调为主导的组织运用模式

以信息协调为主导的组织运用模式,平时建立专门的管理协调机构——“信息资源组织运用管理协调中心”,集中统一组织实施信息资源的管理和组织运用。“管理协调中心”负责平时信息系统的建立、运行的管理和组织与协调工作,并对所属各部队信息资源平时的管理和组织运用提出要求、下达指示。

战时,在各级指挥所的指挥中心内,并行设立专门的信息资源管理协调机构——“海战场信息资源组织运用管理协调中心”,集中统一管理和组织实施战时信息资源的组织运用。“管理协调中心”统一负责战时信息资源的建立、运行、转移、接替的组织运用与协调工作,对所属部队信息资源的组织运用提出要求、下达指示。

这种模式的优点是:平时依托指挥所,便于组织实施信息资源在处置日常勤务和应付突发事件时的组织运用;战时依托指挥中心,可以利用指挥中心掌握战场全局的优势,根据作战需要适时建立信息系统,并根据情况变化实时调整系统状态及工作方式,符合海战场信息资源以指挥控制系统为核心的结构特点。主要缺点是,专设的组织领导机构与

现行海战场信息资源的建设与管理运用由各业务部门按职责分别负责的领导职责不一致,且专设机构中人员的来源广泛,相互协调关系复杂,人员素质要求高。

### 3.3 以资源优化为主导的组织运用模式

以资源优化为主导的组织运用模式,就是以海战场信息资源的优化配置为基本目标,通过对信息资源的有效组织,最大限度发挥信息资源在作战指挥中作用的模式。

这种组织运用模式的优点是,能够从目标优化的角度针对信息资源及其相应“柔性”资源进行综合组织和优化运用,可以在组织运用活动中引入现代运筹分析和优化理论,并通过定量与定性相结合的方法,增强海战场信息资源组织运用的科学性。从未来发展的基本趋势看,以资源优化为主导的海战场信息资源组织运用模式,将成为重要的发展方向。

### 3.4 以目标信息精确指示为主导的组织运用模式

以目标信息精确指示为主导的组织运用模式,就是以组织高效、顺畅的传感器通道为海战场信息资源组织运用的主要任务,以对兵力集团提供精确的目标指示信息为目标的组织运用模式。

这种组织运用模式的优点是,能够有效地将海战场信息资源中的传感器组织起来,围绕信息化条件下作战指挥的关键环节,整合目标信息获取资源,提高对远程目标指示的信息质量,有利信息系统实施近实时的指挥控制,提高对参战各兵力集团指挥控制的时效性和灵活性。

### 参考文献

- [1] 《指挥自动化系统与现代战争》,张树清,金陵书社出版公司,1992.09.
- [2] 《高技术条件的C3I——军队指挥自动化》,刘桂芳,国防大学出版社.
- [3] 《武器和战争的演变》,T.N 杜普伊,军事科学出版社.

### 作者联系方式

通信地址:南京市海军指挥学院  
 邮政编码:210016  
 联系电话:025-80840218



## 第 5 部分

---

# 信息化人才培养与一体化训练

---

# 信息化条件下的一体化联合作战训练

符永健

**摘要：**在信息化条件下开展的一体化、网络化的一体化联合作战训练是各国在进行军事训练转型领域和军事力量转型所面临的重大问题。目前，我军也正在加紧军队的信息化建设与转型的步伐，不可避免的也将面临到军事训练的转变问题。而把传统机械化战争时代的联合训练转型到信息化时代的一体化、网络化联合训练仍然有很多问题需要解决，本文就从美军军事训练一体化、网络化转型的本质和特点入手，初步分析了我军进行一体化、网络化联合训练转型的特点和规律。

**关键词：**一体化联合作战；作战训练；军事转型

军事训练是和平时军队活动的中心工作，也是和平时提高军队战斗力，应对各种复杂、艰苦挑战的重要途径。从军事训练的作用和影响上看，军事训练不单纯是一个训练问题，还是一个基础性、系统性和全局性的军事力量建设问题。通过军事训练的实践活动，不仅可以迅速提高部队的战斗力，而且还可以按照未来战场的实战需要对作战理论、武器装备、指挥控制、后勤保障、编制体制、人才培养进行全面和综合的检验，对军事力量建设的各个领域提出全面的实践需求，牵引和促进军事力量的全面转型。人类进入信息时代后，随着信息技术、网络技术和通信技术在军事领域的广泛运用，现代战争的作战样式向着一体化、网络化飞速发展。为了适应信息化战争作战样式的变革，适应未来信息化战场的需要，各国都在积极地进行一体化作战训练思想、体制和方式的转变。我军一体化作战训练也应当根据未来一体化、网络化作战的战场需求，进行相应的转变，并通过转变促进我军一体化作战理论、武器装备、编制体制等军事领域的转型，提高我军执行信息条件下一体化联合作战任务的综合能力。

## 1 注重一体化作战训练内容向以信息化模拟训练转变

在信息化的战场上，要获得绝对的战场优势，特别是绝对的战场信息优势，不仅需要信息化的武器装备和高性能的指挥控制系统，而且还需要作战人员与武器系统特别是与信息化武器系统之间的完美

融合。要实现这种战场上的融合就必须通过对传统的训练内容进行改革，以信息化模拟训练作为训练的主要内容。信息化模拟训练，以其独特的逼真性、高效性、经济性和安全性，正逐步成为当今军事训练的主流发展趋势。当前，信息技术的迅猛发展和在军事领域的广泛运用，不仅为战争舞台提供了智能化的武器装备，也为军事训练提供了更为逼真、更为高效和更为经济的模拟化手段。

在信息化模拟训练中，参加训练的各个军种和兵种的作战力量，应当能够充分地运用以信息技术为核心的现代模拟技术特别是虚拟现实技术和交互式仿真技术，实现一体化作战模拟训练全领域的虚拟化、模拟化。目前，美军针对其未来作战的需要已经开发了一整套的信息化模拟训练系统，这个系统遍及美军的陆、海、空和海军陆战队的一线作战部队和各级指挥机关，并在其军事院校、训练基地和一体化作战队部中得到广泛的推行，大大提高了美军一体化作战部队的训练水平。在阿富汗战争和伊拉克战争中，美军针对不同的作战对象和作战目的而进行的空中精确打击与特种作战的联合行动、“斩首行动”、“震慑行动”和以地面重型装甲部队快速推进为主的“快速决定性作战行动”都源自美军的信息化模拟训练。未来我军的主要作战样式将是一体化联合作战，为此，我军应当积极地将最新的信息技术成果引入到一体化作战训练的战术、战役和战略等不同层次的领域中去。同时，还应当通过网络技术规范相应的准入技术标准，使这种训练能够在不同的军种内部顺利和有效地实施。

## 2 注重以创新思想为核心进行作战实验与演习

创新是一个民族的灵魂，在军事领域这个最具开放性思想和创新性思想的领域，没有大胆的创新精神和开放型的创新性理念，进行任何军事变革和军事力量转型都将是“一纸空文”，而且没有任何实际意义。这样的思想僵化、默守陈规的军队在未来高智商型的信息化战争中也是毫无战斗力可言的。我军传统的作战训练，主要是采用重复性、检验性和机械化的方法对各种作战部队和武器系统进行相对独立和分立的训练，其主要的功能和作用是巩固军队的战斗力，而对于新理论的创新与研究、完善与改进、检验与推广相对不够重视，训练创新思想往往受固有的训练模式、作战思想和作战方式所束缚，因此，注重克服这样传统训练模式的思维影响是以创新思想指导作战演习与训练的关键。

一体化作战训练作为信息化战争理论和信息化战争样式的创生和演练手段，特别是针对性的作战实验性联合演习，必须要始终把握住创新这个关键性的核心问题。运用创新性的思维，通过作战实验与一体化作战演习，创生先进的信息化作战理论，并再次通过实验把这种本来就在实验室创生的作战理论，使其与武器装备、指挥控制系统、一体化作战部队的编制体制进行初步的磨合，进而对创生的作战理论进行不断的修正，使其能够通过有各军兵种参加的一体化联合作战演习的检验。最后，把其运用于战争的实践，通过战场环境的考验，检验其正确性并调整、改进和推行。可见，在以作战实验室为中心，以军事训练特别是一体化作战演习为纽带，以实战为检验标准的信息化作战理论的创生过程中，创新思维始终占据着重要而关键性的地位。

如果没有创新，就没有信息化一体化作战理论的雏形，也就更谈不上对其进行的修改、检验和推行。当前新军事变革以前所未有的速度迅速发展，机械化战争的形态迅速向信息化战争的形态演变，在这种背景下，军事训练要适应各种战争形态和作战样式的巨大变化，不仅要积极巩固部队的战斗力，而且还要大胆突破常规，将创新性的思维运用于军事训练的转型过程之中，通过训练不断提生作战能力。美军是一支相当注重创新精神的军队，同时美军也相当重视创新精神在作战实验与演习过程中的运用。

美国国防部在 2001 年的《四年防务审查报告》中明确指出：军事转型是一个全面创新性的过程，需要大量反复的作战实验与演示作支撑，而实验则是美军实现军事转型的关键的四大战略支柱之一。在 2004 年颁布的《陆军转型路线图》中，美陆军进一步提出：要最大限度地综合利用战斗实验室、研究实验室、训练与条令司令部分析中心等机构进行实验与演示，以检验和评估部队转型活动是否与目标部队的要求一致。目前，美国陆、海、空、海军陆战队、特种作战部队都有自己的作战实验室，并已经组建了太空作战实验室，通过其创造性的思维和创新性的作战实验，反复组织相应的作战演习，大大提高了美军一体化作战部队的作战能力，为促使美军的军事力量转型的深入发展奠定了坚实的理论和相应的实践基础。美军在作战实验与演习领域的大胆创新及其通过训练催生全新的作战理论、催生部队新的战斗力的方法值得我们借鉴。

## 3 注重向基于能力和效能进行多能化一体化作战训练转变

作战需求是军事训练的直接发展动力，决定了军事训练的模式和发展趋势；而效能的提高则是军事训练的最终目的。机械化战争时期，一体化作战的主要作战样式表现出各军种围绕同一作战目标，进行协同性的作战行动，各军种兵种在力量编成、武器装备、指挥控制、后勤保障、作战行动、战场评估等领域都是相对自成体系的。由于各种标准和规范的不统一，导致了其作战行动中低效能联合，无法形成一个网络化、高度融合的一体化作战网络，各军种武器系统和作战单位的综合作战效能难以得到充分的发挥。在未来的一体化联合作战行动中，各种作战力量都是基于其能力和效能进行的相应行动，通过网络化的战场力量组合模式，充分利用各种可能的战场信息，进行准确、高效和稳定的战场决策，进行实时的一体化联合作战行动，都力求在战场上最大限度地发挥各种战场因素的作战效能。因此，我军在组织一体化作战训练的过程中，必须针对未来一体化联合作战的这个基本特点，基于一体化联合作战部队的能力和效能，对作战部队实施最大限度的多能化训练，以充分提高其实战能力。

目前，由于我军一体化联合作战部队的武器系

统和指挥控制系统，特别是战场通信能力和网络化的指挥控制能力都相对较弱，无法完全实施全方位、全时空、全领域的一体化作战指挥，部队的一体化作战相对于美军来说，仍然存在着巨大的差距。我军在联合训练的过程中，应当针对我军一体化作战部队各种武器系统、作战单位、指挥控制系统的特点和作战目标进行针对性训练，也就是说要基于能力，着重提高我军一体化作战部队的战区海域封锁能力、战区空域的控制与反控制能力、地面部队的战区机动能力以及诸军种联合指挥与信息共享能力等。在训练的过程中，要尽量把我军陆、海、空三军、海军陆战队和第二炮兵部队进行网络化的联合，重点演练如何将其战场感知能力、指挥控制能力、火力打击能力、后勤保障能力、战场评估能力融合为一个网络化的作战整体，使各作战要素能够最大限度地发挥一体化作战效能。

## 4 注重以构建一体化为根本进行联合作战训练转变

在机械化战争时期，联合训练就已经存在，其训练方式、训练思想和训练手段能得到充分的发挥，但是由于工业时代科学技术力量的限制，特别是信息技术的发展和应用水平的限制，即使是像美军这样的军事强国进行的联合作战军事训练在一定程度上来说都是协同性质的，而并非信息化条件下一体化联合作战的样式。在信息化时代，由于信息技术、网络技术和通信技术的飞速发展，在世界军事领域引发了一场深入和彻底的变革。美国于20世纪90年代末提出的网络中心战理论，由于其超前性和先进性，迅速的占据了新军事理论的领先地位

置，并开始引领世界新军事变革的潮流。在网络中心战为主的一体化作战理念的牵引下，美军加快了其信息化建设的步伐，迅速对其指挥控制系统、武器系统、编制体制进行了深入的军事转型。作战体系的一体化、网络化高度联合已经成为其军事转型的基本特征。

目前，美军在构建一体化、网络化联合训练机制中取得了迅速的发展。为了适应美国国家战略调整的需要，美国国防部在《转型计划指南》中明确提出：发展国家联合训练能力的设想，其核心就是通过构建一体化、网络化的联合训练模式，不仅实现陆军、海军、空军和海军陆战队各军种的高度战场融合，而且实现常备力量与后备力量之间、军队与政府部门之间，本国军队与盟国军队之间的全面战场链接。

我军在信息时代也面临着从机械化半机械化军队向信息化军队转变的历史使命，大量先进的作战理念、军事理论和战略思想迅速出现。同时各种先进的武器系统、指挥控制系统迅速装备部队，军队的编制体制也正在进行着一次深入的改革。如何将我军的作战理念、武器装备、指挥控制系统、部队编制体制和一体化作战的具体作战行动进行深入、广泛一体化、网络化的联合，是我军训练转型应当首要面对和解决的问题。因此，根据军事转型的需要，为适应作战思想、作战方式的转型，按照信息化条件下一体化联合作战的要求，依托信息网络系统和指挥控制系统，采取分散配置的方式，把陆、海、空及海军陆战队等诸军种通过指挥控制网和信息通信网进行网络化的联接，实施分布式的一体化、网络化联合训练，应当是我军一体化作战训练转变应追寻的目标。

参考文献（略）

作者联系方式

通信地址：海南省海口市海口警备区

邮政编码：570236

联系电话：0898-66573001

# 适应信息化战争需求突出人才队伍建设重点

李治安

**摘 要：**本文从未来信息化战场需求出发，从人才科技素质、信息化人才培养、人才制度建设三个方面，探讨了对信息化人才队伍建设的途径和手段。

**关键词：**信息化；人才；建设

## 1 前言

随着信息技术在军事领域的广泛应用，一场以信息化为核心的世界新军事变革悄然兴起，信息化战争形态已初显端倪。适应信息化战争需求，培养造就一大批能够推进中国特色军事变革的高素质新型军事人才，既是一项长期的战略任务，也是当务之急。

## 2 突出人才科技素质提高这个重点

在未来战场上，知识对抗将成为军事对抗的本质特征，知识已成为军队战斗力的主导因素和最有活力的增长点。

### 2.1 抓生长干部起点提高

必须适应知识军事时代的需要，在初级军事教育中，技术院校和指挥院校全部实现本科教育。中、高级军事教育应与国家学位教育挂钩，加大军事硕士、博士学位比重。在工程技术院校实行本硕联读和硕博联读制，中、高级指挥院校应适当延长学制，逐步过渡到按硕士、博士的要求培养人才。要瞄准信息化战争需要，站在“明天战争”的基础上进行今天的教育，加大信息化建设与作战理论等“朝阳知识”教学比重，切实解决“培养出来就落后”的问题。同时，应打破学科专业条块分割、内容单一的现状，加大军政兼容、指技合一、文理渗透的力度，使培养的军事人才具有较高的综合素质。要进一步走开依托国民教育培养军队人才的路子。这也是世界各国军事人才的培养趋势。资料显示，美军每年在 400 多所地方大学培养 1.5 万多名军官，占生长干部的 45%，依托培养的高技术人才

也占 30% 以上。目前，我军有近 70 所地方签约高校，已初具规模，应继续加大力度，积极吸纳有志于国防事业的青年学生和专业人才，为科技强军提供不竭的人力资源。

### 2.2 抓在职干部学历升级

学历高虽然不等同于素质高，但文凭学历毕竟是一个人接受高等教育的标志，是知识积累和素质养成的体现。首先，要切实加大军队院校继续教育力度。进一步扩大研究生教育规模，拓宽培训范围，逐步走开在职干部研究生教育培养模式。其次，要扎实搞好“强军计划”实施。充分利用地方高校办学力量，组织干部报考攻读地方大学硕士、博士学位，不断吸收地方高科技最新成果。此外，还要积极鼓励干部通过参加函授、自考等途径提升学历层次，引导他们结合本职工作和部队建设需要，选定学习方向和内容，防止和克服重“包装”轻“武装”，为文凭而学、学非所用，含“金”量、含“军”量低等问题。

### 2.3 抓各类人才知识更新

在信息化领域，知识衰减的速度达到每年 15%~20%，知识的半衰期已缩短至 5 年。我们只有以每年 6%~10% 的速度更新知识，才能跟上时代的步伐。要充分发挥院校培训的主渠道作用，建立健全良好有序的轮训机制，扩大规模、增加数量，使各级各类干部都能及时得到“充电”、“输血”，满足部队信息化武器装备的发展和信息化战争对人才知识结构的需求。要采取“走出去、请进来”的办法，经常聘请军地著名专家学者到部队讲学讲课，积极选派人员到科研机构、工厂见习见学，到国外留学和考察培训。积极营造人人学习、

时时学习、处处学习的良好氛围。

### 3 突出信息化人才培养这个重点

在当前我军积极推进信息化建设步伐的历史时期，必须优先培养造就一批“专家型”、“复合型”、“尖子型”信息化人才，充分发挥其示范带动作用。

#### 3.1 大力培养专家型的研究开发人才

他们是各个信息技术部门从事研究和开发的人才，是信息化人才中数量最少、层次最高的部分。他们应具备技术创新能力，能够时刻掌握世界信息技术的前沿信息，了解信息技术的发展动态，具有灵敏的信息反应能力；能够着眼信息安全、信息作战、信息化战争的需求，研制开发具有自主知识产权的信息技术和设备；能够结合我军武器装备现状，提出以信息技术改造现有武器装备的具体思路和方案，加快我军跨越式发展的速度。这些人才虽然数量少，但地位重要，决定着我国、我军的信息技术发展水平。对这部分人才的培养，主要依靠高等院校、信息科研院所等机构。重点大学和具有培养高水平信息技术人才的研究机构，要重点扶持信息技术相关专业的硕士点和博士点，提高教学水平，改善科研环境，增加招生人数。军工企业要加强与有关高校、研究机构的合作，使研究开发第一线人才的知识不断更新，适应信息技术飞速发展的需要，提高创新能力。

#### 3.2 大力培养复合型的指挥控制人才

他们是信息作战的组织者和指挥者，是赢得信息化战争最终胜利的决策力量。他们应当既通晓信息技术、熟悉信息技术装备和信息网络，又精通信息作战特点和有较强的组织指挥能力；既善于根据上级确定的信息作战决心，具体组织本级信息系统的作战行动，又善于从本级信息系统的技术水平出发，灵活应用信息技术手段，确保信息作战胜利。对他们的培养，院校补训是基础，部队锻炼是关键。要在原来专业培训的基础上，经过信息技术、信息作战、信息指挥控制等新知识、新技术、新理论的补训后，在部队训练、演习等实践中逐步锻炼成长。要进一步增加选送军以上领导干部、师旅级

指挥员、团营职指挥员到相应院校学习信息技术知识、信息作战理论、信息战基础知识，加速复合型指挥人才的培养步伐。

#### 3.3 大力培养尖子型的管理应用人才

他们是将先进的信息技术与设备转化为部队战斗力的主要力量，在未来信息化战争中可以起到千军万马难以发挥的作用。他们应精通信息化武器装备、信息系统设备和信息网络结构的操作、维护和管理，精通网络攻击与防御；具有与信息化战争相适应的信息制胜的新观念和 information 作战的理论水平。对这类人才的培养，主要依靠院校。美国国防部自颁发信息战指示文件后，其国防大学即新成立了信息战争与战略学院，西点军校也开设了信息战争与信息课程，况且美空军在 60 周年庆祝时成立了“网络战司令部”。因此，只有用新的知识体系培养人才，确保我军在未来信息化战争中立于不败之地。

### 4 突出人才制度建设这个重点

培养和造就人才，制度和机制的作用非常重要。优越的人才制度可以吸引人才、激励人才、保留人才。因此，抓人才队伍建设，必须注重在制度创新、完善机制上下功夫。

#### 4.1 要建立和完善人才宏观控制机制

这是保持人才建设正确方向和健康发展的重要保证。一方面，要搞好人才建设总体谋划。十年树木，百年树人。抓人才建设必须有前瞻性和战略眼光，搞好长远规划。要处理好重点与一般的关系，对重点部队、关键岗位和急需人才，做到优先考虑、重点保障、促成优势；要处理好个体与群体的关系，既重视尖子人才培养，又谋求人才队伍整体素质的提高；要处理好眼前与长远的关系，立足我军现状，着眼未来信息化战争需求，分阶段、分层次地搞好人才培养。另一方面，要努力实现人力资源的优化配置。当前，优化配置人才资源的重点和难点是如何加大人才交流力度，通过人才合理流动，最大限度地发挥现有人才效益。领导和机关要克服本位主义思想，树立“大人才”的观念，舍得把组织能力强、用起来顺手、有发展潜力的人才交

流到更多的岗位上摔打锻炼。对一些个人提出的流动要求,只要有利于改善本单位人才队伍结构优化、有利于调动人才的积极性、有利于在更大范围内产生人才效益,就应给予必要的支持。对“只要组织照顾,不要组织纪律”,完全出于个人利益考虑提出的流动行为,要从严控制。

## 4.2 要建立和完善人才考评使用机制

建立科学规范的人才考评和使用机制,能把各级抓人才建设的力量和目标引导到正确的轨道上来,做到准确识人、公正用人,最大限度地激发人才的潜能和活力。要建立公正的考核评价机制,把创新能力、工作能力和实际贡献,作为衡量人才的标准。要紧紧围绕是否有利于战争力增长这个核心,既看人才的学历文凭,又看他们对科技知识掌握的程度,以及用所学知识解决部队建设中的矛盾问题的能力,把人才标准的基点定在“打赢”上。要建立合理的人才使用机制,防止既存在人才匮乏的问题,也有人才浪费、用非所长的现象,使人才有施展才干的平台。要打破人才使用的旧框框,坚持讲台阶而不抠台阶,论资历而不唯资历,要德才兼备而不求全责备,力求做到人尽其才,才尽其用。如对特招入伍的地方大学生,要学会用辩证的眼光看待他们,扬长避短、大胆用才。要建立科学的教育管理机制,坚持以人为本,正确处理严格要求与容短扬长的关系。对“两头冒尖”的人才特别是专业技术人才的管理,既不能一味“哄着来,捧着干”,也不能以行政手段代替思想教育,要以求贤若渴的精神打动人,以礼贤下士的真诚尊重人,以实实在在的行动关心人。要正确运用好奖惩手段,用足用活现有的提前晋职、晋级等人才激励政

策,真正让吃苦者不吃亏,流汗者不流泪,受累者不受气。

## 4.3 要建立和完善人才经费保障机制

近年来,尽管各级加大了人才建设经费投入,但与地方相比,思想还不够解放,步子迈得仍不够大,过分强调以精神鼓励为主的现象还有一定的普遍性。注重精神上的鼓励是非常必要也是十分有效的,我们当然要靠理想信念和崇高的事业吸引和留住大批高素质的人才,但如果忽视了物质待遇,很多工作就会显得苍白无力,正如马克思、恩格斯所说,思想一旦离开利益,就一定会使自己出丑。特别是在社会人才走向市场化的今天,没有相应的物质条件作保障,必定会极大地制约我军的人才建设发展。因此,各级都要进一步强化出人才就是出政绩的思想,学会计算军事人才的投入产出比,舍得在人才队伍建设上多投入。一是在引进和保留人才上加大投入。为了吸收人才、保留人才,就应当注意突出利益原则,给予政策待遇上的保证。二是在培养人才上加大投入。当前,西方发达国家的军队在人才培养上都非常舍得花本钱,如美、法等国家的军队院校,教育经费已占到国防开支的 6%~8%。现在各级经费都很紧张,要办的事很多,但培养人才的经费要给予保障。三是在人才激励上加大投入。坚持按贡献参与分配的原则,敢于打破平均主义,保证冒尖人才待遇上“高人一等”。当前我军实施的优秀专业技术人才岗位津贴、院士津贴等,就较好地体现了这一原则。对出成果、出效益的人才,为尊重其劳动价值,给予回报,进行重奖。在平时要多做“雪中送炭”的工作,及时伸出援助之手,帮助他们解决实际困难。

## 参考文献

- [1] 刘海主编.《军校信息素质教育研究》.北京:军事科学出版社,2006年12月
- [2] 张蜀平主编.《直面信息化战争》.北京:国防工业出版社,2007年1月
- [3] 商则连主编.《国防和军队信息化建设理论研究》.北京:军事谊文出版社,2006年5月

## 作者联系方式

通信地址:西安市沣镐路1号院办空军工程大学电讯工程学院  
 邮政编码:710077  
 联系电话:029-84798405

# 适应新军事变革潮流抓紧工程兵信息化指挥人才培养

徐波 刘军

**摘 要：**工程兵信息化指挥军官队伍建设是工程兵信息化建设的重要组成部分，文章从未来信息化条件下作战对工程兵指挥员的要求入手，分析了工程兵信息化指挥人才应具备的基本素质及目前我军工程兵信息化指挥人才建设方面存在的主要问题，在此基础上，重点提出了加速推进我军工程兵信息化指挥人才建设的具体措施。

**关键词：**工程兵；信息化；指挥人才

工程兵信息化指挥军官队伍建设是工程兵信息化建设的重要组成部分，是未来信息化条件下作战工程保障任务能否顺利完成的关键因素，加快实施工程兵信息化人才培养工程，对于突破工程兵信息化建设“瓶颈”，早日实现工程兵信息化，具有重大而深远的意义。

## 1 信息化条件下作战对工程兵指挥员提出的新要求

### 1.1 工程信息将成为完成作战工程保障任务的基点，要求工程兵指挥员具备强烈的信息意识

随着信息技术的广泛应用，士兵将是综合信息系统武装起来的士兵，武器是信息化的武器，指挥是信息化、自动化的指挥，工程兵指挥员无论是与合成军队的通信联络还是对所属部队的组织指挥，对信息的依赖越来越大。夺取信息控制权和使用权，成为有效遂行工程保障任务的重要保证和战场对抗的焦点。工程兵作为遂行工程保障任务的技术骨干力量，其行动与合成军队行动的联系将更加紧密，信息将成为工程兵组织指挥活动的第一要素。因此，在未来的信息战中，工程兵指挥员必须具备强烈的信息制胜意识，必须自觉做到以信息制约能量、以信息配置资源、以信息沟通指挥、以信息网络化来统筹工程保障任务、以信息来武装军队、以信息战场的要求来更新观念等。

### 1.2 信息主导兵器将成为战场的主宰，要求工程兵指挥员必须掌握渊博的知识

工程装备器材日益自动化、信息化，极大地提高了工程装备器材的性能，不仅伪装器材向综合化、隐形化、智能化发展，地雷战器材向智能化、信息化、空地一体化发展，反地雷战器材也向智能化、综合化方向发展，信息化的工程装备将是工程兵的主要装备。工程兵指挥员能否实现自己的作战意图，参谋人员要及时提出切实可行的建议，政治干部能否展开行之有效的战时政治工作，装备军官能否确保高新装备的有效运转，已经不是以经验来定夺的，而是从根本上取决于他们是否能够驾驭高技术武器装备，把握信息化条件下作战的特点和规律，并在战斗中正确运用。所有这些，客观上都要要求指挥员必须具备现代科学文化知识，既要通晓军事指挥与管理，又要懂得军事科学技术；既要精确的专业理论知识，又要掌握必需的相关知识。

### 1.3 指挥对抗将成为相对独立的斗争领域，要求工程兵指挥员具有很强的协调控制能力

以微电子技术、计算机网络技术为代表的高新技术用于战争以后，不仅拓展了作战空间，提高了兵器打击的力度，而且使战场向一体化发展，使作战单元对指挥控制的依赖越来越大。作战指挥系统结构更加复杂，其功能也得到极大的发展，指挥机构的生存面临更加严峻的挑战。特别是电子领域的斗争，有可能使军队的“神经系统”瘫痪，使力量优势的一方因指挥无力而变为劣势。指挥将从传统的运筹帷幄的“后台”，走向与敌直接对抗的“前



台”。工程兵作为战斗保障兵种，不仅要适时调控内部的工程保障行动，而且更重要的是要适时根据合成军队的变化调控自行的行动。因此，在未来的信息战中，工程兵指挥员必须具备很强的协调控制能力，在激烈的对抗当中、在战场节奏快速转换过程中，辨别真伪，定下正确的决心。

## 2 我军工程兵信息化指挥人才建设现状

近一段时间，随着我军工程兵信息化建设步伐的不断加快，信息化指挥人才队伍建设也在稳步推进，应该说，成效比较明显。主要表现在：院校“主渠道”的地位更加突出，干部岗前培养的路子已经全面走开，干部交流力度不断加大，但也存在着不少问题。一是思想观念的落后影响和制约着工程兵信息化指挥人才队伍建设，还在自觉不自觉的沿用机械化战争时代的思维方式和观念，来指导信息化指挥人才的培养。比如，受惯性思维影响，院校教育理念、办学思想、教学内容更新、教学方法手段运用等方面，不能完全按照信息化的要求来组织教学，学员的学习效果自然也不会太好。二是信息化条件下作战对人才的要求与当前我军工程兵指挥人才队伍建设现状差距较大，目前存在着“两低、一少”的状况。“两低”指学历层次低，虽然我们近几年加大了改善人才队伍的学历结构的力度，但与西方发达国家相比，我军目前军官的学历层次还是较低的；信息素养低，主要表现在我军目前的指挥员对信息化武器装备使用、管理等的掌握不够，特别是工程兵是一个专业多、武器装备多、技术含量较高的兵种，更需要我们的指挥员具备较高的信息素养；“一少”指任职经历少，虽然前一段时间我们在干部的岗位交流上下了一些功夫，但由于各种原因，干部交流制度还没有完全走开，直接表现为目前工程兵部队指挥员任职经历单一，很难适应未来信息化条件下作战的要求。三是信息化指挥人才生成渠道不畅。主要是：从部队内部培训来看，工程兵部队驻地分散，任务繁重，难以组织大规模、长时间的集中培训，容易导致培训的不规范、不系统、不经常，增加了信息化人才培养的难度。从院校培养体系来看，现有院校的专业设置还不能满足培养信息化人才的需要，信息化知识教学的比重也相对偏低。从借助地方资源来看，受社会

大环境影响，加上部队人才政策机制的相对滞后，对人才的吸引力明显不足，在一定程度上形成了“需要的进不来、进来的用不上、用上的留不住”的不利局面。

## 3 我军工程兵信息化指挥人才建设的对策

### 3.1 加强工程兵信息化指挥人才建设的宏观谋划

良好的顶层设计对信息化人才建设可以起到事半功倍的效果。具体来说，一是要从规划上统筹。认真落实军队信息化建设规划和工程兵部队人才建设规划，准确把握人才成长的客观规律，既要考虑当前急需的信息化人才培养问题，又要考虑中、长期信息化人才培养问题，努力形成一支既满足当前急需又能适应未来发展的信息化人才队伍。二是要从结构上统筹。依据现有岗位和工作需要，科学确定信息化人才队伍规模，统筹各类人才进出的具体要求和指标，确保信息化指挥人才个体素质良好，整体结构优化，进出更替有序，使之与工程兵部队建设相一致，与岗位需要相协调，与肩负使命相适应。在大力引进高层次信息化人才的基础上，盘活现有人才，通过有序流动、科学配置、优化组合，追求现有信息化指挥人才效益的最大化。三是要突出信息化条件下应急作战工程兵指挥人才培养。应急作战军事斗争准备是我军当前最紧迫、最重要的战略任务，为此，我们在关注人才队伍整体建设工程的同时，更应突出应急作战指挥人才的培养，对于应急作战工程兵指挥人才而言，必须针对应急作战工程保障的特点和要求，采取超常规的方法，构建工程兵信息化指挥人才培养的“快车道”。

### 3.2 拓宽工程兵指挥人才培养渠道

一是充分发挥好军队院校作为培养新型军事人才的“主渠道”作用。军队院校是培养信息化人才的基地。应通过深化教学改革、优化学科专业结构、完善信息化教学内容体系、健全淘汰制度等措施，促进工程兵指挥人才成长。在人才培养观念上要实现院校人才培养的“三个转换”：即单一结构型向复合结合型转换；知识型教育向能力型教育转换；课堂理论教学为主向课堂加模拟教学转换。在

教学内容上注重强化“三贴近、一更新”，加大信息化教学内容的比重，不断构建“新、精、实”的内容体系。在教学方法手段上，要不断加大信息化手段建设及应用力度，突出网络化、研讨式教学。二是积极探索院校、部队、科研机构联合培养模式。院校应该通过有计划地组织教员、学员到部队调研、实习和代职，主动了解未来信息化作战对人才素质的要求，学员岗位任职所必需的知识和能力，特别是要了解新装备发展趋势、部队训法及战法改革实际，为其科研、训练提供人才与技术支持。部队应该通过选派经验丰富、素质高的优秀干部到院校介绍部队情况或任教，为院校输送优秀业务骨干充实教员队伍。三是走开依托国民教育培养军队人才的路子。开放式培养军事人才，是世界各国军事人才培养的一个趋势，也是我军培养高素质军事人才必须实行的一个带方向性的重大政策。目前，我军已经迈开了依托国民教育培养军事人才的路子，应该继续拓展军事人才的培训渠道，不拘一格吸纳人才，特别是要与地方高等院校、科研机构加强双向交流，大力开展开放式教育，吸收有志于国防事业心的青年和具有工作实践经验的专业人才，使这些人才资源成为科技强军的强大的支撑力量。

### 3.3 注重工程兵指挥人才育人环境建设

育人环境建设要“两手抓，两手都要硬”。一方面，要创新信息化指挥人才培养机制。要通过创

新评价机制，积极吸纳先进的人才评价理念，从基础入手研究建立以基本标准、专业标准、层级标准为内容的综合评价体系，将信息素养作为官兵素质的重要组成部分。通过创新考核机制，建立科学的考核指标体系，并实行党委统一领导下的职能部门与群众考核相统一的考核机制，促使信息化人才增强内在动力，不断积极进取。通过创新选拔机制，坚持重实绩、重公论，重素质，以实践为标杆，以能力论英雄，任人唯贤，唯才是举，不拘一格选拔和任用人才，进一步形成尊重知识、人才辈出的生动局面。另一方面，不断完善信息化的指挥人才训练平台。目前，我军工程兵信息化指挥训练平台建设已经取得了一些成果，比如，《工兵团（旅）指挥训练模拟系统》、《舟桥团（旅）指挥训练模拟系统》、《工程兵参谋技能训练与考核系统》等，这些成果已经在院校与部队训练当中发挥了很好的效能，但与信息化条件下作战对指挥系统功能的要求相比还有一定的差距。我们必须在这些现有平台的基础上，按照未来信息化战争怎么打，人才就怎么培养的思路，不断完善指挥训练系统信息获取、传递、处理等的功能，把工程兵指挥人才放到近似实战的信息环境中进行锻炼和考验，通过网上推演、网上作业、网上训练、网上对抗等方式，切实使工程兵部队指挥员掌握信息作战的基本理论、作战原则和主要战法，全面提高工程兵指挥员打赢信息化战争的能力。

### 参考文献

- [1] 刘鹏主编，《走向军事网格时代》。北京：解放军出版社，2004年版
- [2] 郭牧主编，《外军部队数字化建设与发展研究》。北京：解放军出版社，2002年版
- [3] 许震和主编，《作战方式的革命性变化》。北京：解放军出版社，2004年版

### 作者联系方式

通信地址：江苏徐州工程兵指挥学院

邮政编码：221004

联系电话：0516-83150105    0516-83150401    13852001020

# 信息化军事人才的心理素质培养

吴耀光

**摘 要:** 本文从价值观念培养、智能品质培养情绪情感品质培养等方面分析了信息化军事人才心理素质培养的内涵,从注重心理选拔,加强心理学知识教育等诸方面探讨了信息化军事人才心理素质培养的主要途径和方法。

**关键词:** 信息化; 军事人才; 心理素质培养

## 1 前言

信息化战场的比拼是信息化人才的较量,毫无疑问,着眼未来战争需要,培养信息化军事人才将是我军建设和发展的关键。因此,培养大批适应信息化作战需要的高素质信息化军事人才是目前院校教育的当务之急。信息化军事人才心理素质的培养是一个复杂的系统工程,需要正确把握信息化军事人才心理素质培养的内涵,研究探讨科学有效的培养途径和培养方法,并运用于信息化军事人才心理素质培养的具体实践过程中去,这样才能真正提高信息化军事人才的心理素质。

奉献,因而对其价值观的要求也就非常高。故此,我们提出把信息化军事人才的价值观念作为其心理素质培养的首要问题,绝不是信息化军事人才心理素质培养问题上贴的一枚政治标签,它是既符合人的心理素质结构的科学性,也符合我军信息化军事人才的素质结构特殊要求的。

## 2.2 智能品质培养

信息化军事人才的智能素质是由认知、思维、记忆、想象、操作等多种品质构成的多层次复杂结构,在这一结构中,创造力是其发展的最高层次和境界。“为创造性而教”,已成为当代教育发展和人才培养的重要思想。在信息化军事人才的智能素质中,创造能力应该成为最重要的素质。美国将军巴顿说:“战场几乎没有任何一种情况是教案上和演习中所见过”,21 世纪的战场情况将更是难以预料的。跨世纪的信息化军事人才必须具有创新意识、创新思维和创新能力,才能自觉地排除干扰,创造性地预测、评价复杂多变的战场情况,及时定下正确的决策,运用高超的谋略、新奇有效的战法克敌制胜,始终把握住战场的主动权。因此,部队、军事院校的教育训练必须把加强军人创造性培养放到重要位置,使信息化军事人才学会学习,善于自主学习,勇于探索新知识,强化创新意识,提高创新能力。

## 2.3 情绪情感品质培养

信息化军事人才,其情绪稳定与否,对军事行动的影响更为巨大。在未来信息化战争中,战场情况复杂多变,战争中充满着艰苦和危险,还要面临敌方强大的心理战攻击。心理素质良好的信息化军

## 2 信息化军事人才心理素质培养的主要内涵

心理素质培养的蕴涵十分深厚,根据现代教育理论关于人的全面和谐发展的要求和我军信息化军事人才的培养目标,依据科学心理学的原理,信息化军事人才的心理素质培养应重点抓好以下几个方面:

### 2.1 价值观念培养

以理想、信念、世界观为核心的价值观念体系,是人心理结构中的统驭和调节系统,居于心理结构的最高层次。信息化军事人才价值观念培养的主要内容包括共产主义理想,社会主义的信念,热爱祖国和人民的情感,献身国防事业的无私奉献精神以及辩证唯物主义、历史唯物主义的世界观等。军人的职业又是充满艰苦、紧张和危险的事业,它需要军人忍受难以忍受的痛苦,做出无私的牺牲和

事人才应该具有稳定的情绪,始终保持清醒的头脑,具有很强的控制情绪的能力,在任何情况下,都应是胜不骄、败不馁,临危不惧,处变不惊,措置若裕,保持积极稳定的情绪。因此,培养信息化军事人才良好的心理素质,必须重视抓好情绪情感品质的教育培养。

## 2.4 意志品质培养

顽强的意志品质是走向卓越的心理基础,是心理素质良好的主要表现,集中反映了军人不怕艰难困苦、奋勇拼搏、夺取胜利的恒心和毅力。在革命战争年代,毛泽东同志一贯要求人民军队的指挥员要有坚强的战斗意志,要发扬坚毅顽强的战斗精神,要有威武不能屈、困难吓不倒、失败不气馁的百折不挠的性格,“不论在任何艰难困苦的场合,只要还有一个人,这个人就要继续战斗下去。”中国革命在艰苦恶劣的条件下之所以取得了世界瞩目的胜利,是与革命先烈英勇顽强的战斗意志紧密相关的。

加强信息化军事人才意志品质的培养,是未来信息化战争的客观要求。战争既是物力的较量和智力的角逐,又是作战双方意志的抗衡。高技术局部战争中,军人的意志将面临严峻的考验。

## 2.5 性格品质培养

人改造环境,环境也塑造人。信息化军事人才的特殊社会角色,对其性格也提出了特殊的要求。古今中外的大量事实证明,在一定条件下,将帅的性格,往往成为战争胜负、国家存亡的决定性因素。我国古代军事家孙臆早已指出:作为统兵的将帅如果妄自尊能、骄傲自满、轻举妄动,或者缺乏勇气、迟疑不决、意志懈怠,必然导致战争失败。性格品质上的这些缺陷愈多则危害愈大。良好性格品质的培养,是信息化军事人才心理素质培养的一个必不可少的重要内容。

# 3 信息化军事人才心理素质培养的主要途径和方法

信息化军事人才心理素质培养,是关系到我军质量建设的重要课题。对我军来说,信息化军事人才的心理素质培养尚是一项具有开创意义的工作,

还没有多少成熟的经验可以借鉴,需要在不断探索中前进。我认为,应该把信息化军事人才的心理素质培养作为一个系统工程,不仅要把它纳入教育训练的渠道,使它进入教材,进入课堂,进入训练场,而且要把它同思想政治教育、部队管理和陶冶养成教育紧密结合起来,渗透于我军建设的各个层面,使之成为我军质量建设的有机组成部分。其中最重要的,是抓好如下几个方面。

## 3.1 注重心理选拔,确保信息化军事人才的心理质量

良好的心理素质,是高素质信息化军事人才成长发展重要基础。因此,我们要借鉴外军的有益经验,重视信息化军事人才的心理选拔,严把信息化军事人才的心理质量关,防止基本心理条件不适合的人员进入部队或作为信息化军事人才提升使用,保证信息化军事人才的心理质量。为此,应做好如下工作。

一是统一思想认识,确立对军人进行心理选拔是培养高素质信息化军事人才,加强我军质量建设的重要措施的思想,为信息化军事人才的心理选拔做好思想舆论准备。

二是开展军人心理测量、选拔的研究。运用军事心理学、军事医学等相关科学理论,研究军事活动与各种心理品质的相关度,确定一般军人、各特种兵员、特殊信息化军事人才必备的心理品质要求,制定诸如新兵、军校学员、领导干部和某些特殊信息化军事人才的相应心理测量标准,研制科学的心理测验工具,为信息化军事人才的心理测量、选拔提供科学的理论和方法。

三是建立对信息化军事人才进行心理选拔的机制,形成不经心理选拔就不能进入各种信息化军事人才队伍的制度。

要逐步开展对应征青年、特种兵人员、新入学的军校学员、预提升使用军官的心理测查,通过全面了解其认知、感情、意志、个性心理品质状况,对其心理素质作出慎重、严格和科学的评价,做到对信息化军事人才的心理品质心中有数,知人善任。要把心理素质状况作为选拔信息化军事人才的一个重要指标,对有严重心理障碍以及有可能形成心理疾病潜质的人,都不应征集入伍、选拔入学或作为担当作战指挥重任及特种信息化军事人才的选拔对象。通过建立信息化军事人才心理选拔机制,

实施严格的心理选拔,为我军信息化军事人才的选拔培养提供良好的心理基础,以适应新时期军队建设和未来高技术局部战争的客观要求。

## 3.2 加强心理学知识教育,把信息化军事人才心理素质培养建立在坚实的理论基础之上

信息化军事人才良好心理素质的培养,最基础、最根本的一点就是要大力普及心理学知识。要重视研究青年官兵心理特点,要求各级领导和政治干部学一点管理学、社会学、心理学等方面的知识。这对于我们在部队开展心理学知识的普及教育,探索和研究信息化军事人才心理素质的培养,具有重要的指导意义。

### 3.2.1 把心理学知识教育作为教育训练的重要内容

院校是培养信息化军事人才的基地,在培养高素质信息化军事人才方面发挥着极其重要的作用。应该说,在和平时期,我军军官、特别是生长军官的基本素质,是在院校奠定的。现在的军校学员,将是二十一世纪我军建设的骨干,军校学员应该具备良好的心理品质。但根据我们的调查,当前军校学员的心理健康状况却非常令人担忧。因此,要把军校学员的心理教育作为重点抓好。总政和总参联合发出《关于加强和改进院校政治理论课教学的若干意见》的文件,规定在院校的不同对象中要分别开设《军人心理学》、《思想政治工作心理学》两门课程。这就第一次以法规的形式把心理教育纳入了我军院校教学的课程体系。我们认为,根据当前我军心理教育的发展状态,全军各级各类院校都应开设相关的心理学课程,真正使心理教育进入教材、进入课堂、进入生活,把心理教育作为素质教育的突破口,以促进军校学员整体素质的全面发展和提高。

### 3.2.2 编写心理素质教育的教材

为满足信息化军事人才心理素质教育的需要,必须编写出适合信息化军事人才阅读、有利于信息化军事人才心理素质培养的高质量的教材。目前,我军心理教育教材的编写应注意如下一些问题:一是要有利于心理学知识的普及;二是要区分层次,不搞一刀切;三是教材编写的科学化。

### 3.2.3 培养一批心理教育的人才

由于心理教育的专业性、知识性和科学性要求较高,而我军心理教育普及性不够,能够进行心理教育的人才十分缺乏。为了不使我军的心理教育在低水平上徘徊,必须培养一批思想品质良好、热爱心理教育、有较高心理学知识修养和教学能力、有一定实践经验的专门人才,以推动我军心理教育向更高层次发展,深化我军信息化军事人才心理素质的培养。从我军当前的实际出发,心理教育人才的培养可从以下渠道进行:一是我军院校直接培养;二是进修和委托培养;三是直接引进

## 3.3 强化心理训练,提高信息化军事人才心理适应能力

根据当代信息化战争的特点及其对军人心理素质的要求,借鉴外军的经验,我军信息化军事人才的心理素质训练应从如下一些方面着手。

### 3.3.1 近似实战训练

军事心理学研究表明,军人训练的环境越近似实战,其表象就越正确,就越有价值,就有助于培养军人适应战场环境的心理素质。因此,进行训练,必须从实战要求出发,有意识地创设逼真的战场环境,设置近似实战或高于实战的高强度、高难度科目,在近似实战的环境条件下摔打部队,全面提高军人的心理素质。

### 3.3.2 战场模拟训练

模拟的内容通常包括战场境况和战斗困难情境的模拟两个方面。可以建立模拟训练场和计算机模拟室,通过模拟高技术战场的外部景象和复杂的战斗情景,模拟战场上可能出现的各种复杂、多变、危险情况,把官兵置于近似实战的模拟环境之中,让其了解、熟悉现代各种兵器的战术技术性能、对手的战术技术特点,探索应对敌信息化战争的方法对策,增强克敌制胜的信心;利用战场模拟系统,让其目睹或体验“战场”的“实际”情况,使官兵亲身体验战场环境刺激和战时的心理状态,使之经受心理考验,提高经受各种刺激的心理阈限,增强其对信息化战争战场环境的心理适应能力,逐步学会自我调节,增强心理调节能力,提高心理活动水平,以适应现代战争的战场环境。

### 3.3.3 野战生存训练

野战生存训练是军人适应性训练的一项重要内容，它不仅可以提高军人在恶劣的自然条件下的生理适应能力，而且还可以在严峻的战场困难环境中磨练军人的胆量、意志，增强军人的心理耐受力 and 坚韧力。野战生存训练既可以单独专门进行，也可以结合演习演练综合进行。训练方式要活，训练内容要全，既合理又带冒险性。通常的做法可以是：将部队综合编组，空投到自然条件恶劣的孤岛、沙漠、戈壁、海上、高山雪原、热带丛林，置于酷暑、严寒或危险、困境之中，严格限定时间，使受训官兵独自一人或几人在极为孤立、毫无外援、水断粮绝的环境中求生；还可以结合战术演习设置复杂多变的敌情，增加艰难危急的战斗情节，使受训官兵的心理素质及生存与作战能力在作战任务艰巨和生存困难的双重威胁下进行锻炼和提高。

### 3.3.4 心理调控训练

每个人的心理素质都是不尽相同的，而且一般都存在这样或那样的心理弱点，这都可能成为信息化军事人才在平时工作或战争条件下的心理隐患，

这就需要重视抓好心理调控训练。所谓心理调控训练，就是运用科学心理学的原理，根据现代战争的要求，通过专门编写的“心理训练想定”，对信息化军事人才进行知、情、意的全面训练，使他们熟练掌握和运用心理调控方法，善于调节和控制不良心境，进而提高适应和处置战场上可能出现的各种复杂情况的能力和自我心理恢复能力。若条件允许，可以建立心理训练实验室、训练基地等，对官兵进行普遍轮训。

## 4 结束语

人的各种素质的发展，都是以心理素质为基础和中介的。信息化军事人才的心理素质是其整体素质结构中不可或缺的重要组成部分，而且在很大程度上影响和制约着其他素质的形成和发展。本文提出要培养信息化军事人才良好的心理素质，这是针对培养对象的心理特点，培养我军高素质信息化军事人才的重要内容，是适应新军事革命要求，立足于打赢未来高技术局部战争，加强我军质量建设的重要课题。

## 参考文献

- [1] 侯喜贵主编，《军队信息化建设研究》. 北京：国防工业出版社，2007年1月
- [2] 刘海主编，《军校信息素质教育研究》. 北京：军事科学出版社，2006年12月
- [3] 商则连主编，《国防和军队信息化建设理论研究》. 北京：军事谊文出版社，2006年5月

## 作者联系方式

通信地址：西安市沣镐路1号空军工程大学电讯工程学院训练部

邮政编码：710077

联系电话：029-84798407

# 关于加强军校研究生信息素质教育的思考

孙继银 何芳芳 王园

**摘要:** 信息化战争催生信息化军队, 军校建设信息化无疑是新军事革命对军校建设提出的新要求, 而我军研究生的信息素质与这种必然要求还存在着一定的差距。本文明确了军校研究生信息素质教育的内涵, 并在此基础上提出了加强军校研究生信息素质教育的一些可行性办法。

**关键词:** 信息化战争; 军队建设信息化; 军校研究生; 信息素质教育

## 1 信息素质的内涵

信息素质是一种判断、获取、评价和利用信息资源能力的综合表现, 包括信息理论知识和信息实践能力两个方面。军队院校信息素质是我军高素质军事人才信息素质的集合, 而军事人才信息素质就是指军事人才适应信息时代需要, 在信息社会中获得信息、利用信息、开发信息, 应对信息战争等方面所应具备的修养与能力。主要包括以下三方面。

### 1.1 信息意识教育

信息意识是指对知识信息的本质及功能的认识, 是指对知识信息重要性的认识和对知识信息的敏感程度, 即人们从信息的角度对社会中各种现象、行为的感受、理解和评价这种自觉的对信息的心理反应。信息意识教育目的在于激发个体潜在的信息需求意识, 并能充分地正确地辨析和鉴定信息的价值, 合理地利用信息, 从而形成一种对信息敏锐的思维感知能力和对信息所特有的恒久注意力。

### 1.2 信息能力教育

信息能力教育是信息素质教育的主要方面, 包括信息认知能力、信息获取能力、信息处理能力、信息利用能力四个方面。

1) 信息认知能力。它是信息获取、整理、处理、利用、交流的开端, 具备良好的信息认知能力, 才能处理好信息的质与量的关系, 这是在网络时代能妥善处理爆炸性信息的关键。

2) 信息获取能力。包括信息技术的应用能力、信息的查询、获取能力, 是及时、有效地获取本学科领域内的相关信息以及有关社会生产所需的

各类信息的能力。

3) 信息处理能力。是指在信息获取的基础上, 结合专业知识进行分析、判断, 使信息有序化、专业化的能力, 是信息组织、加工、分析能力的综合体现。

4) 信息利用能力。认知、获取、处理信息的最终目的在于达到信息资源的有效利用, 体现信息资源的价值, 是信息素质中最重要的能力之一。

### 1.3 信息道德教育

信息道德是调节信息生产者, 信息传递者信息使用者之间相互关系的行为规范, 信息道德教育可以促使人们在信息活动中遵循一定的信息伦理与道德准则, 规范自身的信息行为。在信息技术高度发达的未来社会, 不良信息泛滥及信息侵权行为时有发生, 信息犯罪也不可避免, 所以信息素质教育应该加强信息道德教育, 避免在未来实践中发生不必要的纠纷。军校信息素质是社会信息素质的一部分、同样要求军人须遵循一定的信息伦理和道德准则, 按照国家和军队的有关规定, 规范自己的信息行为。

## 2 加强军校研究生的信息素质教育是军校建设信息化的当务之急

### 2.1 军校研究生信息素质的现状

信息化战争催生信息化军队。未来的信息化战场, 信息知识将由潜在的、间接的战斗力的跃升为现实的、直接的战斗力的。军校建设信息化无疑是新军事革命对军校建设提出的新要求。而我军官兵的信息素质与这种必然要求却存在着巨大的差距。一是

信息意识淡薄。突出表现在信息化战争意识模糊和信息制胜观念不强两个方面。在相当数量的官兵头脑中对信息化战争的概念、样式都是模糊不清的,更谈不上信息制胜观念的强烈。二是信息知识匮乏。主要表现在信息技术知识和信息战知识两个方面。许多官兵还不甚了解信息技术的基本常识,对信息系统的结构组成及工作原理知其然不知其所以然;对信息技术的作用与影响,认识也并非特别深刻;对信息战的构成要素、作战原则、作战目的似懂非懂;对网络战、电子战、情报战、心理战知之甚少。三是信息能力不强。主要表现在信息系统的使用能力和信息能力两个方面。网络环境改变了军人获取知识信息的传统方式,数字图书馆、网络教学,使不具备信息能力的官兵感到纷繁复杂,不知所措。相当一部分官兵不会操作信息系统,更谈不上用军事专用网络系统平台完成网上作业想定;不会使用数字化战场的各种信息设备,更谈不上对信息战的谋划、组织、指挥、抗干扰等。

## 2.2 信息素质是军校研究生必备的素质

研究生群体是军校中最渴求信息的群体之一,研究生要撰写论文,要进行科学研究,就必须大量阅读各类藏书、浏览网络各类信息,这就要求研究生具备一定的信息素质,更好地搜集信息、鉴别信息、选择信息、利用信息,有效地开发各种信息资源,这样更能创新,并将成果转化为我军的现实战斗力。

上述种种情况,必然要求加速加强信息素质教育,提高我军官兵的能力水平,否则,别说“打赢”,甚至连参战的资格都没有,只能任人宰割。我军现在还处在“组建数字化部队”阶段,离“信息化军队”的要求还差之甚远。“数字化装备”可以买得来,但具备信息素质的军人却买不来。没有良好的信息素质的军人,即使有精良的“数字化装备”,也很难发挥出应有的战斗力,再先进的计算机网络,也很难发挥其应有的作用!目前全军院校人才队伍的数量规模、能力素质、知识结构等,与担负的特殊使命任务、与建设信息化部队、与打赢信息化战争的要求还不相适应。因此,提高军校研究生的信息素质就成了军校建设信息化的必要前提、迫切要求、当务之急。

## 3 加强军校研究生信息素质教育的方法

进入知识经济时代,无论是发达国家还是发展中国家,都把加快推进信息化作为跨世纪的战略任务。发达国家在推进信息化进程中,重视信息基础设施建设同时,也充分认识到公民信息素质的重要性。美国是最早开展公民信息素质教育的国家,其信息素质教育在研究中不断发展,在具体实施中不断完善,给我们带来了诸多的启示,正所谓“他山之石,可以攻玉”,借鉴他们的成功经验,有助于我们开展军校研究生信息素质与能力培养的研究。

### 3.1 加强军校信息素质教育的理论研究,促进教育广泛开展

系统的、科学的、先进的理论体系可以促进实践活动的开展。我们需要尽快创建一套具有我军特色的、完整而系统的信息教育理论体系,包括学校教育教育与终身教育、自我教育与强制教育。研究人员将在把握信息技术与信息基础知识共性的基础上,借鉴发达国家的理论和经验,充分考虑我国的文化传统及价值观念、经济模式与发展水平、政治结构与法律机制,结合我军院校的信息化发展的整体态势与时代要求,既面向世界又立足本国,来审视信息道德、信息价值、信息法律、信息安全等问题,以适当超前的精神来阐述概念、概括规律、观测动向,保证理论能够发挥对实践的指导和促进作用。

### 3.2 对军校生信息素质的内涵探讨及标准制定,教育目标定位明确

对应于军校研究生信息素质的内涵而言,军校生的信息素质主要包括知识、意识、能力三个层面。军校生知识层面的信息素质包括信息知识、信息安全知识、信息战知识三个方面。信息知识主要指信息技术的基本常识、信息系统的结构与组成、信息系统的工作原理、信息技术的作用和影响等;信息安全知识指对信息实施安全管理的技术和措施等确保军事信息的保密性、完整性、可用性、可靠性和可控性的知识;信息战知识指了解信息战的定义及实质,了解各种信息战的主要用途和作战目的,了解网络战、电子战、情报战、心理战等信息战的基本样式,明确信息战的原则和信息作战的构



成要素,能熟练运用与自身作战任务相关的信息战基本战法和有关信息攻防手段等。军校生意识层面的信息素质包括信息意识、信息安全意识、信息道德意识三个方面:信息意识指信息军事条件下的战争观以及坚定的信息制胜观念,强烈而明确的信息需求和较高的信息敏感性;信息安全意识指信息安全关系国家安全、战争胜负的观念,信息安全法规意识等;信息道德意识指正确认识信息技术的作用,具有高度的社会责任感和良好的网上军人形象等。军校生能力层面的信息素质包括信息系统使用能力、信息能力、信息战能力三个方面:信息系统使用能力指正确无误地操作信息系统,使用军事专用网络系统平台完成网上作业想定和作战指挥,熟练使用数字化战场的各种信息设备等;信息能力指以各种形式发现、评价、利用和交流信息的能力,即信息获取能力、信息理解能力、信息处理能力、信息利用能力、信息创造能力等;信息战能力指信息战谋划能力、信息战组织能力、信息战防御能力和信息战抗干扰能力等。

通过对军校生信息素质的定义及内涵的探讨,以及信息素质能力标准的制定,可以使教育目标定位明确,并为信息素质的评价及信息素质教育评估提供依据。军校的信息素质教育要以社会道德、法律意识和创造性能力的培养为核心,强调信息技术以人为本的方法论和创新意识,注重人文和社会因素,所培养的信息素养人(Information Literacy Person),要求具备的不仅包括利用信息技术和信息资源的能力,获取、识别、加工处理和创造信息的能力,更重要的是以自主学习的态度和方法、以批判精神及强烈的社会责任感和参与意识,并将他们用于实际问题的解决和进行创新性思维的综合信息能力。

### 3.3 在实践中完善对军校信息素质教育的研究

军校也可以通过一些切实可行的实验项目的开

发及实施,卓有成效地推进信息素质教育实践的开展,经过不断的试验,积累丰富的经验,在实践中逐步完善。

1) 军队院校要成为这个实验平台的关键支撑。军队院校必须按照军队信息化建设和打赢未来信息化战争的要求,适时调整专业学科体系、教学体系,突出信息化特色,不断加大信息科技知识的教学内容,构建电子信息、计算机科学技术、信息安全等贴近未来信息作战和部队信息化建设需要的学科群。充分利用院校的军事理论和战法创新基地来研究部队信息化建设问题,在解决这些问题的实践中,培养和提高军校研究生的信息化素质。

2) 构建全军院校开放式网络资源平台。近年来,全军院校建设多媒体教室 1000 余个,建成了各院校的校园网和第一条覆盖全军的军事训练信息网,实现了全军院校的互联互通;实施了数字图书馆建设工程,集成信息资源总量达 4 万 G,相当于 5 千万册;集中开发了虚拟实验室系统,研究生运用电脑即可进行各种仿真模拟实验;启动了现代远程教育,部分院校多个专业开始招生培训,信息化教学平台初步形成。但这些只是初步解决办法,相对于全军军校研究生来讲,还远远不够。因此,要设法构建全军院校开放式网络资源平台,让军校研究生都能充分实现网上的研究型学习、开放性交流、模拟化演练。

3) 构建多级信息作战实验室和作战模拟中心。院校要分层次建立信息作战实验室和作战模拟中心,充分运用信息作战模拟训练系统,以虚拟现实技术构造信息作战战场,让院校研究生都来充当各级指挥人员,与作战对手进行信息作战、网上对抗实战演练,达到提高军队信息素质的目的。

总之,只有提高军校研究生的信息素质,使之具有适当的信息学理论知识和水平,具有信息认知、评价、利用的能力,才能与军队信息化建设的进程相适应。

### 参考文献

- [1] 刘放.论军队信息素质与战斗力,《湖南社会科学》,2005.4.
- [2] 杨自娟.我国研究生信息素质教育初探,《甘肃科技》,2005.8.

### 作者联系方式

通信地址:西安市第二炮兵工程学院 402 教研室 邮政编码:710025 联系电话:13468971571

# 适应新军事变革努力锻造高素质信息化人才

汤宁 张波平

**摘 要：**根据新时期军事斗争准备要求，结合信息化在现代战争中的主导作用和我军信息化人才建设现状。本文从信息化人才在未来军事斗争中的重要性等方面进行了深入的探讨，针对新时期我军不断加强信息化人才建设及应该特别关注的问题，提出了可资借鉴的对策建议。

**关键词：**新军事变革；军队信息化；人才建设

信息化战争，装备是基础，人才是关键。在未来信息化战场上，知识将成为战斗力的主导因素，敌我双方的较量，将突出表现为高素质人才的较量。当前我军正处在从机械化、半机械化向信息化过渡的时期，加强信息化人才建设十分重要。我们必须强化“高素质人才是打赢信息战争保证”的观念，努力培养、造就大批德才兼备的高素质信息化人才，为军队信息化建设提供强有力的人才和智力支持。

## 1 信息化人才在军队信息化建设中的重要性

一是信息化人才是军队信息化建设的关键要素。军队信息化的实质是在军队建设的各个方面应用现代信息技术，深入开发、广泛利用信息资源，加速实现军队现代化的进程。信息技术和信息资源是由人来研究、开发和创新的，其与军队各个方面的结合也是靠人来实现的，军队信息化建设各个要素自身的发展，也都需要多门类、多层次、高水平人才的支持。美军的信息化建设之所以走在世界的前列，正是因为其拥有占有优势的高素质信息化人才，其他各世界军事大国也无不把信息化人才培养放在军队信息化建设的首位。因此，实现军队信息化的前提是加速实现人才的信息化，信息化人才是军队信息化建设的根本要素，对军队信息化其他各要素的发展速度和质量有着决定性的影响，是军队信息化建设的关键。

二是信息化人才是军队信息化建设的根本保证。军队信息化建设的高速发展，需要大批高素质的信息化人才。美军认为，决定其军队信息化建设速度与质量的最重要因素是拥有高素质的人

才。当前广泛存在于发达国家军队和发展中国家军队之间的“数字鸿沟”，在很大程度上也是源于信息化人才数量的多少和素质的高低，“信息化人才是最宝贵的资源”已成为共识。随着我军信息化建设的深入发展，对各类高素质人才的需求将会更加迫切，只有重视和加强信息化人才的培养，加快全军广大官兵的信息知识和信息技能的普及和提高，才能从根本上提高军队信息化的建设速度。

三是信息化人才是打赢信息化战争的决定性因素。随着以信息技术为核心的现代高技术的迅猛发展，集当代科技成果于一体的信息化武器装备大量应用于现代战争。许多信息化武器装备的功能越来越强，甚至可替代人的某些脑力劳动，但信息化武器装备并不能替代信息化人才的智慧，信息化武器装备的发展，只不过是人的能力的延伸，丝毫没有降低人的因素在战争中的作用。技术先进的美军，尽管装备一流、信息化程度极高，但却更加重视人的作用，其现役军官 98%是大学本科，80%具有硕士以上学位，为了适应信息化作战指挥的需要，他们通过层层筛选，使各级指挥机关中的程序设计专家占 30%，作战运筹和指挥自动化管理专家占 30%，大量掌握现代信息技术的高素质官兵，已成为美军战斗力的重要构成要素。这些都启示我们，知识就是力量，人才就是战斗力，在未来的信息化战争中，谁抢占到信息人才这个“制高点”，谁就能在战场上取胜。

## 2 信息化人才的结构现状

近年来，面对信息化战争的发展趋势，全军各部队都对信息作战理论进行了比较深入的研究和探讨。但是，由于受各种因素的影响，官兵知识结构

与信息化战争的要求还有很大差距,信息化建设与信息化人才的矛盾异常突出,严重制约着部队信息化建设发展和信息作战研究的进程。主要表现:

一是信息作战理论薄弱。信息化战争要求实现每位军人的信息化,使每个军人都具备一定的信息技术和信息网络知识,能够熟练地操作使用手中的信息化武器装备和信息设备,成为信息化条件下的合格战士。而当前部队对这个问题的认识还有一定差距。作战部队官兵大多奔波于传统条件下的训练场,忙于训练、管理、勤务工作,对信息技术和信息网络知识重视不够,对新战场、新战法的研究不够深入,因而,信息作战理论比较薄弱,成为亟待解决的问题。

二是文化素质参差不齐。信息化人才,应该具备一定的学历层次,掌握一定的社会基础科学、自然科学和信息技术、生物技术、新材料技术、新能源技术、航天技术、海洋开发技术的高科技知识。但当前部队实际却很不容乐观,学历层次普遍偏低,干部中以大专、中专为主,战士中以初中、高中为主。虽有相当数量的官兵通过各种途径获得了高学历文凭,但其“含金量”不高,相当数量官兵拿到的是经济、法律甚至医学方面的高学历,对本职工作没有多大的帮助。还有部分官兵,虽然学历较高,但工作经验很少,工作能力非常弱,也无法担负重任。

三是知识结构单一。部队军政指挥军官,因受兵种专业、职能分工、训练大纲及保障能力的制约,知识结构单纯,业务技能单一,难以适应信息化战争的要求。不少指挥员对常规作战特点和战法有比较深入的研究,但对信息作战理论、信息技术装备、信息网络技术了解不深,综合素质不高。也有部分技术院校毕业的军官,经过院校系统学习,有一定的信息技术基础,但指挥能力又很弱。

四是创新能力较弱。部分领导同志创新精神不够,思想保守,因循守旧,没有为部队创新人材营造一个良好的环境。相当部分军官缺乏创新意识,不思进取,安于现状,对信息化装备的开发和运用不积极,对新战法、新训法的研究不深入,没有敢为天下先的勇气与信心,没有强烈的事业心和责任感。

五是培养渠道狭窄。长期以来,我军绝大多数军官出自军队院校,受选材范围,院校培养名额、办学投入、师资力量、生源质量等因素的制约,军

官培训数量非常有限,这与我军信息化建设和打赢信息化战争的要求相比,有相当大的差距。干部毕业后,接受继续教育的机会很少,知识无法更新,跟不上发展的形势。虽然当前部队中很多干部为提高学历参加了自学考试,但大多是经济、法律方面的,对本职工作无甚帮助。

### 3 信息化人才培养的措施对策

军队信息化是一项基础性事业,对人才的需求是空前的。这就要求在发挥军事院校人才培养主渠道作用的同时,拓宽人才培养的路子,多方式、多手段、多层次、全方位地造就一支信息化人才队伍,确保军队信息化建设持续、高效、健康、有序地发展。

一是在部队建设中,着力提升官兵的学历层次。首先把好兵员质量关,达不到高中学历的青年不准入伍,逐步实行大学毕业生必须到部队服兵役的制度,实现兵员文化层次的飞跃。其次,要严把提干关,达不到本科以上学历者不作考虑,实现军官文化层次的飞跃。再次,要把好军官晋升关,无优异业绩者不晋升。逐步扩大从研究生中选拔领导干部的比例,努力提高连以上军官的学历层次和实际水平。

二是在院校教育中,努力提高培养军官的起点。要着眼信息作战需要,以师、团、营职军官为重点,以本科教育为起点,着重加强信息作战指挥人员的培养力度。学习信息作战基本理论、信息作战技术理论及信息作战应用理论等知识,形成与信息作战相适应的军事观念,提高军事理论水平;熟悉信息作战武器装备的战术技术性能,提高综合运用信息作战武器装备的能力;进行谋略战例研究、想定作业训练及运用计算机模拟、沙盘作业等手段进行的谋略实施训练,提高信息作战指挥人员的谋略思维能力;组织进行战场信息环境分析、敌我信息作战能力分析及制定信息作战计划等训练,提高信息作战指挥人员的组织指挥能力,锻造具有复合素质及应用能力的信息作战指挥人才。

三是坚持持续培养,重视高层次人才交流。坚持持续培养是指各类人才从院校毕业后继续进行的岗位培训。既可由本单位指定有专长的人或邀请专家组织教学,也可组织人员分批入校轮训,巩固提高在校学习的成果,弥补因信息技术发展迅速而导

致的知识和技能不足。使人才的培养由一次教育变为多次教育；由在工作中学习变为不断进修提高；由忽视任职前教育变为重视岗位培训，以增强信息化人才培养的连续性和学习内容的系统性，提高实际工作能力。同时还应重视建立高层次人才交流机制，解决好人才逆向流动、基层高学历干部缺乏、配置不够合理等问题，提高人才使用效益。

四是实施开放办学，拓宽人才培养渠道。信息技术具有军用和民用双重性质，为军民结合培养信息化人才提供了客观可能性。因此，为加速我军信息化人才培养，可从以下三个方面着手。一是面向社会，与地方联合办学，直接从地方高校信息技术专业毕业生中选拔军官，或委托有条件的地方高校为部队代培专门人才，逐步解决军队培训力量不足与部队需求较大的矛盾。二是根据作战需要，有计划的组织军队干部到地方信息网络基础设施参观见学，与地方高校、科研院所和信息产业部门进行合作开发，增长信息专业技术知识，加快锻炼和提高的步伐。三是抓住国家改革开放的宝贵时机，加强与外军的交流与合作，适时酌情加大出国进修深造的干部数量，或聘请外籍信息作战的专家来我军讲学授课，开阔我军信息化建设及其信息作战研究的视野，丰富和提高我军的信息作战知识和信息作战理论水平。

## 4 加强信息化人才队伍建设应把握的几个问题

当今世界，随着知识经济的逐步形成和新军事革命的迅猛发展，全球信息化浪潮涌动，以信息技术为核心的高新科技已经成为生产力提高、战斗力增强的决定性因素。高科技信息化人才作为掌握和运用科学技术的主体力量，其地位和作用更加明显。

### 4.1 加强组织领导，创造拴心留人的环境

建立一支高层次信息化人才队伍，必须营造适合人才健康成长的良好环境。一是优化政治环境。强化广大干部特别是各级领导干部的人才意识，将抓高层次人才队伍建设的成效，作为党委班子和领导干部政绩考核的重要内容；大力宣扬先进典型，弘扬高层次人才的爱国主义精神、爱岗敬业精神、

求实创新精神、拼搏奉献精神和团结协作精神；珍视高层次人才取得的实绩和成果，并通过不同形式予以认定和表彰，进一步激发他们的成就感和事业心；牢固树立“爱才用才、树才聚才”的观念，形成尊重知识、尊重人才的良好风尚。二是优化工作环境。干事业、出成果，既是我们吸引和保留高层次人才的根本目的，也是他们自身的目标追求。科学调配、合理使用，将高层次人才恰当定位，积极为高层次人才创造发挥聪明才智的机会，提供施展才华的舞台，积极发挥高层次人才的群体效能，大力开展科研协作，努力改善办条件，保证为高层次人才提供必要的设备和仪器仪表，发展以计算机远程联网检索、光盘检索、多媒体视听为代表的新技术情报检索手段。三是优化生活环境。努力改善物质生活条件是稳定高层次人才队伍行之有效的重要措施之一。应始终把解决高层次人才的实际困难和做好生活服务保障工作，作为加强高层次人才队伍建设的大事来抓。对事关高层次人才生活方面的事，要努力做到心想到、话说到、力尽到、事办到，用真情温暖他们。主动关心高层次人才的家庭困难，想法设法解决其家属子女就业就学等方面的后顾之忧，保证高层次人才全身心地投入工作。

### 4.2 正确合理使用，建立有利于高层次信息化人才生长的运行机制

一是任用机制。逐步实行学位与职务挂钩。院校和科研单位聘任的中级技术职务者一般应具有硕士学位。聘任的高级技术职务者一般应具有博士学位；信息化部队主官和作战部门领导，军以上单位信息化机关指挥和参谋人员，院校机关教学管理人员，应逐步具有硕士研究生以上学力。二是竞争机制。制订高层次人才考核标准，对他们进行公开、公正、科学的考评，真正做到优者上、劣者下，强者上、弱者下，走开能上能下的路子，激发上进，鼓励冒尖。严格实行专业技术职务的任期考核制度，对高级专业技术职务人员，一个任期之后必须重新参加相关职务的评审，通过评审后方可续聘。三是保留机制。加强思想政治工作，大力宣扬先进典型，弘扬他们献身国防、爱岗敬业、拼搏奉献的精神；改善工作环境，用事业留人；增加相关岗位，用政策留人；改善生活条件，用环境留人；优化人际关系，用感情留人。加大高层次人才在军内的有序流动，做到人尽其才；对确实不适宜在军队

工作高层次人才，要及时流动出去。四是提高机制。有计划地组织有关人员进修深造、学术交流、出国考察，以开阔眼界，拓宽思路。实行继续教育制度，在通信院校中设立各类人才培训中心，采取进修班、短期培训、集训等多种形式，定期对高层次指挥军官和技术干部进行轮训，促进其知识更新。

#### 4.3 注重选拔培训，造成适应军事通信发展需要的高层次信息化人才群体

高层次信息化人才，在我军通信人才队伍建设和信息化建设中具有举足轻重的地位和作用，要适应“两个根本性转变”，必须加大选拔培养力度，努力建设适应军事通信发展需要的高层次信息化人才群体。高层次信息化人才群体包括军政合一、指技合一的复合型指挥人才、能参善谋的智囊型人才、专家型的技术保障人才、熟练掌握装备的骨干人才。一是建立和完善培训机制。结合高层次信息化人才队伍建设，建立和完善一套严格正规的培训

办法，对培训的数量、专业、目标、培训周期做出明确的规定。把出国深造、国内学者访问、在职攻读学位、学术“疗养”、聘请讲学等学习深造的有效形式加以条理化、制度化。利用有利条件，适时举办各种高新技术学习班、研讨会；经常开展跨大单位联合重大科技攻关，以促进高层次信息化人才培养。二是拓宽引进渠道。加大从地方引进高层次人才的力度，建立人才举荐网络，持之以恒地做好高层次人才的发现、联络和引导工作，鼓励各级单位和个人积极推荐人才，对引进人才成绩突出的，及时予以奖励。采取聘请客座教授、邀请讲学、开展科研项目合作等有效措施，积极引进智力资源，促进高科技人才队伍建设。三是加强政策引导。对高层次人才应具备的资格和水平做出明确的规定和要求。把学习深造的经历和成效以及学术研究成果作为考核的重要内容。特别对高级专业技术职务干部每年应发表学术论文的数量和质量，要有明确的规定，以改变目前学术研究水平不高的状况，推动高层次人才的培养和提高。

#### 参考文献（略）

#### 作者联系方式

通信地址：云南省昆明市金碧路 77200 部队 13 分队

邮政编码：650032

联系电话：0871—4770306

# 立足推进军事训练转变加强士官教育训练信息化建设

王存才 钱叶平 张文武

**摘 要：**新世纪新阶段推进机械化条件下军事训练向信息化条件下军事训练转变，是我军信息化建设的时代要求。士官人才是我军战斗力建设的基础，在士官教育训练中，坚持以信息化建设为牵引，全面扎实推进教育训练改革创新，是实现军事训练转变的重要一环。本文重点对士官教育训练中的观念转变、体系构建、模式手段创新等进行了深入细致的研究。

**关键词：**军事训练转变；士官教育训练；信息化建设

深入贯彻落实全军军事训练会议精神，推进机械化条件下军事训练向信息化条件下军事训练转变，是我军信息化建设的时代要求。士官人才作为我军战斗力建设的基础，在其教育培养中，坚持以信息化建设为牵引，全面扎实推进教育训练改革创新，铸就适应信息化战争需要的合格士官人才，是推进军事训练转变的重要一环。

## 1 着眼军事训练转变目标，更新信息化士官人才培养理念

军事训练转变第一位的是思想观念的转变。转变的进程就是不断解放思想、更新观念的过程。着眼建设信息化军队、打赢信息化战争需要，必须用信息化人才培养理念牵引士官人才队伍建设，推进士官教育训练的创新与发展。

### 1.1 遵循信息化士官人才培养原则

当前，我军建设总体上还处于机械化半机械化阶段，现阶段的建设重点是以信息化牵引机械化，完成机械化向信息化建设的跨越发展。为此，推进士官教育训练改革创新，着力培养信息化士官人才，必须立足实际，着眼长远，遵循以下基本原则。

#### 1.1.1 基础性原则

在信息战这一全新的作战样式中，影响部队战斗力效能的关键因素，是军事人才快速灵活、抢占先机的能力和素质。培养信息化士官人才亦不例外，必须从高处着眼，从基础入手，立足于信息化

建设的客观需求，切实抓好士官体能、智能、技能和心理攻防训练，打牢信息化建设基础。

#### 1.1.2 实践性原则

士官人才是高技术武器装备的操作、维护和管理者，实操技能要求高，应进一步加大实践环节，充分运用设置近似实战的网络环境和训练环境，突出现代虚拟技术、模拟技术和实装实弹训练，培养士官人才的综合信息素质。

#### 1.1.3 创新性原则

信息化建设给部队的作战任务、作战方式、编制体制等均提出了很多新的要求，也赋予了部队训练以新的内容和形式。与此同时，信息技术的飞速发展及其在军事领域内的广泛应用，也要求我们不断更新观念，拓展思维，创新训练方法手段，以便为部队输送更多的信息化士官人才。

### 1.2 创新信息化士官人才培养观念

信息化程度的提高主要依赖于观念体系的转变。要深入开展信息化条件下的教育训练，首先必须树立与信息时代要求相适应的教育训练思想，确立以打赢信息化战争为牵引，以高新技术知识为基础，以专业理论知识为核心，以新型信息系统武器装备为重点的科学合理的士官人才培养理念。一是树立正确的信息时代观念，增强全体人员在整个教学过程中重视信息、研究信息、利用信息的紧迫感。二是树立先进的信息人才目标和质量观念，拓展士官人才信息能力培养的内涵及外延，培养知识、能力、素质全面发展的人才。三是更新和完善教学基本理论，以信息化的教学方式促进传统教学

效益的提高,促进教学系统的整体优化。

### 1.3 强化士官教育训练大系统意识

推进士官教育训练创新,必须摆脱条块分割、自成体系、政出多门、各自为战的羁绊,确立一体设计、上下贯通、左右协调、整体发展的士官教育训练大系统观念。一是推进军事训练转变,“五支队伍”建设必须齐头并进,特别是在军队信息化程度越来越高、武器装备发展越来越快的情况下,越是要建设一支高素质的士官人才队伍。二是士官人才培养作为一项系统工程,培养信息化士官人才,必须充分发挥各承训单位的教育训练资源优势,针对人才的知识、能力和素质需求,搞好顶层设计,构建分工合理、上下衔接、全程培养的一体化培训体系。三是确立院校、训练机构、部队、科研院所、装备生产厂家之间的系统协作观念,实现信息互通、优势互补,拓展联合培训渠道,促进系统优化和协调发展,真正做到全程育人、合力育人。

## 2 适应军事训练转变要求,构建信息化士官人才培养体系

推进军事训练转变,形成一体化联合作战能力,必须加快军事训练向信息化聚焦,构建信息化条件下士官人才教育训练的科学体系,实现教育训练的实战化、科学化和正规化。

### 2.1 拓展士官人才培养目标的新内涵

在未来高新技术密集、对抗领域广阔、作战进程迅速、形态复杂多变的信息化战场,士官除了应具备基本的政治素质、操作技能、管理能力之外,还必须具有一定的智能对抗能力,真正成为“信息化”士官。因此,在构建士官人才培养目标时,应把信息化知识与信息化素养作为其重要内容。“信息化”士官人才的特点主要体现在三个方面:一是具备基本的信息技术知识。即着重掌握计算机、网络、电子、通信技术、自动控制技术等知识,强化信息技术,打好信息化基础。二是具备信息化装备操作技能。信息化在某种程度上就是“自动化”、“智能化”、“网络化”、“一体化”。士官作为武器装备的直接操作和使用者,在未来信息化战争中,既要正确执行上级命令,又要迅速准确地完成操作

和灵活机动地排除故障,以确保高技术武器装备最大效能地发挥作用。三是具有较高的信息素养。即具有获取信息、利用信息和处理信息的能力,熟悉信息化的学习、生活、工作和战争环境。

### 2.2 深化教育教学内容改革

培养适应部队信息化建设需要的士官人才,应立足部队信息化建设实际,优化课程设置,加快教学内容改革。一是加强物理、电工、电子、计算机等工科专业的基础教学和实验教学,增加与信息化武器装备操作、维护和管理密切相关的微电子、卫星通信、仿真等内容,打牢士官信息素养及其岗位创新能力培养的知识基础。注重学员科学思维方法的培养,加强其对知识的创新与运用的综合训练,努力实现传授知识、培养能力和提高素质的有机结合。二是紧跟部队信息化建设步伐,通过外聘专业人员、开展讲座、参观展览等形式,及时将新的信息化装备、信息化战争的基本作战理论、外军信息化建设的成果与趋势等,及时传授给学员,使其不仅掌握信息化武器装备,熟悉部队应对信息化战争的训练方式和作战方式,而且了解外军信息化建设进程,增强信息化建设的使命感、责任感。三是整合教学内容,在传统课程中补充信息化内容,增设《信息战概论》、《新装备知识介绍》等课程,突出新知识、新装备、新技术、新战法在课程教学中的地位,并实时动态更新,以“信息化”促进传统课程的提升,提高教学的先进性和适用性。

### 2.3 动态优化士官专业体系

信息技术的飞速发展,高新技术在军事领域的广泛运用,武器装备信息化水平的不断提高,以及信息化战争作战样式的不断创新等,均对士官人才培养的专业体系建设提出了新的更高要求。一是增加信息知识含量,提高专业信息化水平。我军坚持机械化、信息化复合式发展,现有的士官人才专业建设应紧跟高精尖武器的发展,加大现有装备的信息化改造力度,将当代军事、信息技术的前沿知识融入到教学中,使专业内涵不断拓展。二是针对信息化建设需求,增设新专业,形成信息技术优势专业群。专业设置既要适度超前,体现先进性和时代性,又要切合部队建设实际,按照“贴近士官、综合优化、满足急需,兼顾未来”的原则,充分吸纳

一些信息化水平较高、发展较为成熟的专业，充实到士官人才专业建设中，使士官专业建设形成教学观念先进、教学力量雄厚的专业群，以带动整体信息化建设能力的提高。

### 3 坚持信息主导，逐步推进士官教育训练转变

推进信息化条件下的士官教育训练转变是培养信息化士官人才的关键环节。为此，必须紧紧围绕信息化士官人才培养目标，突出士官学员专业技能和教学信息化建设，扎实推进现代化教学工程，真正做到“出好人才、多出人才、快出人才”。

#### 3.1 提高信息化教学水平，构建开放协作的教学模式

要充分发挥校园网信息化建设的“前哨”作用，实现课程讲授、教案辅导、课外咨询、资料查询、问题解答、探讨交流、学术研究等全程教学功能，满足“分布交互式”的教学需求；要逐步加快士官继续教育步伐，不断完善函授、自考、在职培训等教育形式，积极开发士官远程教育系统，面向部队基层实施远程教学；要着眼于信息技术的军地通用性，适应军队信息化建设步伐，有效实施开放办学，充分利用地方的师资、设备、设施等资源，完成士官人才部分信息技术的讲授、实作和实习任务。

#### 3.2 突出岗位综合技能培训，深化教学内容改革

深化士官教学内容改革，必须在突出针对性和适应性上狠下功夫。要瞄准武器装备型号和部队作战需求，分类别、分层次、模块化构建士官培训课程体系；要按照模块化、综合化、专题化教学设计思想，大力加强综合课程和实践课程建设，制订完善新型课程标准；要跟踪新技术、新战法、新训法的发展变化，增加信息知识、信息技术、信息装备等内容；要突出信息化武器装备应用和管理能力培养，建

设特色鲜明的立体化、信息化士官教材体系。

#### 3.3 坚持“以人为本”，改革教学组训方法

在士官教育训练中坚持和体现“以人为本”思想，就是要以强化学员职业技能、提高学员全面素质为根本目的，全方位展开教学方法创新行动，逐步形成观念先进、特色鲜明的教学方法体系。为对，必须运用信息化教学手段，从传承型教学向开发学员潜能、培养其创新思维的创新型教学转变，实施多媒体教学，充分发挥其“变静为动”、“变抽象为具体”、“变复杂为直观”的特性，大力推广启发式、研讨式、自主式、学导式等先进的教学方法，强调从“教为中心”向“学为中心”的转变，实现教学与导学的统一，注重培养士官学员学习知识的方法和研究解决问题的思路。

#### 3.4 加快信息环境建设，促进教学保障能力跃升

要按照“一体化、集约化、信息化”的要求，加快信息环境建设步伐，不断提高信息化教学保障的综合能力和效益。针对信息化士官人才培训中装备教学的短板，全面分析士官教学训练模拟器的需求状况，科学制订建设规划，合理划分各士官培训单位训练模拟器研制任务；充分发挥院校、部队和装备生产厂家等单位的各自优势，加大训练模拟器建设力度，逐步提高装备教学能力；统一标准和要求，积极构建士官培训网站体系，开发现代远程教育训练软件系统，以专业课为重点，建设一批精品网络课程和教育训练资源库，坚持建用并举，逐步完善，促进现代化教育训练保障能力的整体提高。

综上所述，立足推进军事训练转变，加强士官教育训练信息化建设，是适应军队信息化建设，加紧军事斗争准备，快速培养信息化士官人才的必然要求。作为士官承训单位，只有坚持以信息化建设为牵引，更新培训理念，优化培训体系，创新培训方式，全面扎实推进士官教育训练转变，才能培养和造就大批高素质信息化士官人才。

参考文献（略）

作者联系方式

通信地址：安徽省蚌埠市燕山路 1454 号海军蚌埠士官学校训练部

邮政编码：233012

联系电话：0552-4679140



# 新型军事指挥人才模型建构及培养对策

孙海成 林华生

**摘 要：**本文着眼未来信息化战争特点和我军建设发展战略要求，突出新型军事指挥人才模型建构及培养对策问题，分析了新型军事指挥人才素质能力要求，建构了新型军事指挥人才培养目标模型，提出了新型军事指挥人才培养的对策措施。

**关键词：**信息化；新型军事指挥人才；培养

胡主席强调指出：“努力造就大批适应军队信息化建设、胜任信息化条件下作战任务的高素质新型军事人才，是加速推进我军信息化建设的关键。”胡主席的重要论述，深刻阐明了高素质新型军事人才的内涵，揭示了高素质新型军事人才培养与推进我军信息化建设的辩证关系，为谋划信息化条件下我军指挥人才队伍建设指明了努力方向。新型军事指挥人才培养，必须着眼未来信息化战争特点和我军建设发展要求，科学构建人才目标体系，完善培养战略策略，努力探索一条符合我军实际的指挥军官素质能力建设之路。

## 1 新型军事指挥人才的素质能力要求

信息化战争与机械化战争不同质的特点，要求军事指挥人才具有不同质的素质能力。这些不同质的素质能力，实质是新型军事指挥人才适应信息时代军事变革和军事创新实践活动所必须具备的特殊素质能力。

### 1.1 对军事指挥人才个体的素质能力要求

未来信息化战争，对军事指挥人才个体的素质能力，要求在具备传统的军政融合素养、指技合一素养、军兵种兼通素养、复杂环境适应素养外，还应特别具备以下四种信息素养。一是善于运用战场信息进行调兵用兵的能力。信息化战争，信息成为重要的战略资源，成为战斗力的核心要素。在战场上，信息流控制着物质流和能量流，引导着火力流和兵力流。指挥员要想正确用兵、合理布势，必须首先学会正确分析判断各种信息，善于运用战场信息筹划作战，指挥作战，调兵遣将。二是善于运用

电磁环境进行布兵设阵的能力。机械化作战，指挥员习惯于根据地理环境布兵设阵。但信息化条件下，影响兵力兵器发挥的主要因素已由地理环境位移至电磁环境。如果周围电磁环境复杂并不能得到有效控制的话，将直接影响作战兵器特别是精确制度导兵器的发挥。这就要求指挥员要了解电磁环境构成要素，熟悉复杂电磁环境对作战的影响，战时心中必须装有两个态势图：一个是基于地理环境的敌我兵力对比态势图，一个是基于电磁环境的敌我频谱对比态势图。要熟悉电磁频谱特性，具备善于运用电磁环境布兵设阵、调兵遣将的能力。三是善于运用信息系统实施组织指挥的能力。机械化作战中，指挥员通常是沙盘前论兵、电台前调兵，依靠通信兵实施作战指挥。而信息化作战中，通信、情报、气象等保障人员将逐步走向后台，指挥人员将逐步走向前台，通过辅助决策系统在大屏幕前论兵，利用未来指挥平台和机动指挥控制系统直接实施作战指挥。这就要求指挥人员要了上述系统的操作使用方法，能够熟练运用这些系统实施作战指挥，四是善于管理控制信息战场的能力。信息化作战较之机械化作战，主战场由地理战场位移至信息战场。战场构成要素也随之发生了革命性变革，信息网络、电磁频谱、战场信息成为信息战场的主要构成要素。美军在海湾地区并没有完备的地理战场，但却能接连打败伊拉克军队的重要原因，是其有比较完备的信息战场。信息战场是全新战场，具有与地理战场完全不同的管理理念、管理模式、管理手段、管理标准。要求指挥员必须了解信息战场、熟悉信息战场，具有善于管理控制信息战场的的能力。

## 1.2 对军事指挥人才队伍的素质能力要求

未来信息化战争对军事指挥团队的素质能力要求,突出在三个方面:一是有效掌控战局的素质能力。我军信息化条件下的作战,是捍卫国家主权和领土完整的正义之战,但也客观地受着国际环境诸多因素的影响和制约。作战目的的有限性和制约因素的多重性,要求我们由基于大规模火力取胜,向精确取胜、快速取胜和以小的代价取胜转变。要准确了解敌情,准确判断强敌介入和国际社会反应程度等等,有效把握作战强度、打击力度和行动节奏甚为关键。不具备掌控战局的素质能力,是不可能取得作战的整体效果。二是遂行任务决策的素质能力。信息化条件下作战是以行动为中心的精确作战,要求指挥员必须改变“拍脑袋式”的决策方式,善于运用辅助决策系统,依托专家队伍进行科学决策;改变“长官式”的决策模式,充分调动各级的积极性、创造性,鼓励和采纳创新建议,实现民主决策;改变地图前分析、沙盘前论兵、会议桌前定决心的断续式决策程序,运用电子地图、电子情报、态势屏幕和指挥终端,实施分布交互同步式决策,实现战役战术灵活性与战略决策坚定性、战争的持续性协调统一。三是临机实时指挥的素质能力。信息化条件下的精确指挥,要求实现作战指挥信息流程的快速循环。在陆、海、空、天一体化作战中,各级指挥机构和各类指挥终端都是网络化战场上的一个个节点,要求指挥员熟练运用指挥终端,对各节点的兵力、兵器实施网络化指挥。信息化战场情况瞬息万变,要求指挥员对各种作战单元和作战武器平台实施临机实时指挥,创造性地发挥指挥效能,快速形成优势态势。在信息作战中,要求指挥员充分有效利用信息,加速“侦察、判断、打击、评估”循环,通过隐真示假、以少示多、以无示有等方式,扰乱和降低敌人的认知和行动循环,取得不战而屈人之兵、少战而屈人之兵、巧战而屈人之兵的效果。

## 2 新型军事指挥人才培养目标模型建构

科学的培养目标,应该是新型军事指挥人才素质能力结构的直接体现,是知识、技能和能力所组成有一个多序列、多要素和多层次的动态综合系

统。从信息化战争对军事指挥员的素质能力要求看,新型军事指挥人才的培养目标模型主要有基础能力、专业能力和指控能力三个层面复合构成,并且是一个开放式的动态综合系统。

### 2.1 基础能力层

基础能力层,是指新型军事指挥人才认识事物、解决问题和创造活动的能力。这种能力通常也称智力,智商高低是衡量智力水平的一个标准。基础能力,通常包括观察能力、记忆能力、思维能力、操作能力、应变能力、评介能力、心理能力、体能等,它们组成了一个有机的智力结构系统。一般来说,基础能力又是以学历教育程度为标志。不同的学历间接标志着智力开发的不同程度,尤其第一学历是标志智力高低的重要依据。较强的基础能力,是军事指挥人才能力建设的基本特征。对于新型军事指挥人才来说,衡量其基础能力的高低,重在选拔,次在补差,关键在于具有自我完善能力。

### 2.2 专业能力层

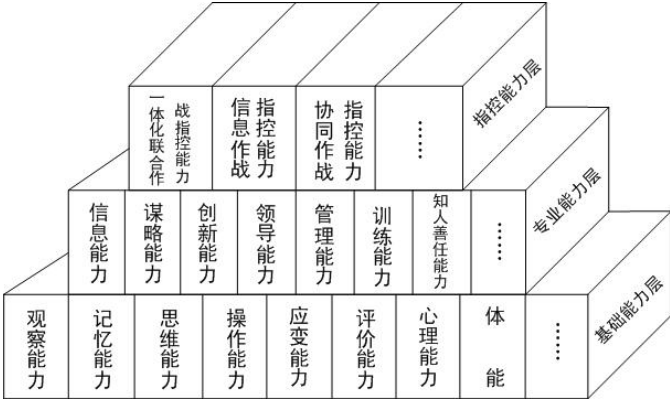
专业能力,是指新型军事指挥人才顺应新军事变革、我军信息化建设和胜任本职岗位所必需的多种能力有机结合成的专业才能,是在基础能力之上形成的赖以应对现实挑战的能力。它是由信息能力、谋略能力、创新能力、领导能力、管理能力、训练能力、知人善任能力等组成,其中信息能力、谋略能力和创新能力相对成为专业能力建设的新核心。信息能力,主要包括强烈的信息意识、较高的信息技术水平和科学利用信息的方法。谋略能力,主要指具有政治远见和军事全局的谋划驾驭能力。创新能力,主要指顺应信息时代和新军事变革趋势,推动军事理论和实践创新的能力。较强的专业能力,是新型指挥人才素质能力的重要特征。

### 2.3 指控能力层

指控能力,是指新型军事指挥人才胜任信息化条件下作战任务和打赢未来信息化战争的军事指挥能力。未来信息化战争是体系与体系的对抗,诸军兵种一体化联合作战是最基本的作战样式。新型军事指挥人才必须着眼一体化联合作战指挥需求提升作战指挥能力。主要包括四个方面:即以指挥信息系统为平台的指控能力、以联合指挥体制为依托的

指控能力、以情报信息为主导的指控能力和以作战行动为中心的指控能力。信息作战是未来一体化联合作战的重要组成部分，新型军事指挥人才必须着眼信息作战的特点提升指控能力。我军正处于由机械化半机械化向信息化建设发展的转型阶段，协同作战指挥能力高低也是影响未来战争态势和战争胜

负的重要因素。概括起来说，新型指挥人才指控能力集中体现在一体化联合作战指挥能力、信息作战指挥能力和协同作战指挥能力这样三个方面。较强的指控能力，是新型指挥人才能力建设的时代特征。



新型军事指挥人才培养目标结构模型

3 新型军事指挥人才培养对策措施

当前我军信息建设加速发展和军事斗争准备的紧迫形势，要求我们必须把新型军事人才的素质能力培养放在在重中之重，采取超常的措施与办法，有战略、有重点、有步骤地取得突破性提升。

3.1 抓紧完善培养战略策略

按照军委确定的人才战略工程总要求，着眼履行我军新的历史使命和打赢信息化条件下局部战争的要求，抓紧修订和完善新型军事指挥人才的培养战略。在此基础上，形成“三种类型”、“两个阶段”的培养行动策略。“三种类型”，即着眼战略、战役和战术级作战指挥人才需求，构建起谋划型、计划型和执行型的新型军事指挥人才教育培养目标。“两个阶段”即以 2010 年前为第一阶段，主要实施“重点培养”工程，对应急作战部队军政指挥员实施逐批轮训，4 年内实现普遍轮训 1 次；对重点部队团以上军政指挥员实现 3 次以上培训，即交叉培训、联合培训和出国培训各 1 次；对其他部队军政指挥员进行“苗子”选拔培训。第二阶段从 2010 年开始，全面实施“精英培养”工程，选拔优秀军政指挥员进行全维度、全过程培训，力争在 2020 年前，达到“培养和造就一支具有战略眼

光，能够把握世界军事发展趋势，懂得信息化战争指挥和信息化军队建设的指挥军官队伍”的目标。

3.2 加速军队院校职能转型

新型军事指挥人才的素质能力培养，主要途径是军队院校和部队实践活动。军队院校作为新型军事指挥人才培养的主渠道之一，必须加速以课程内容改革创新为中心的教育转型发展，按照战略、战役和战术三类新型军事指挥人才，全面构建新型知识结构和能力训练的教育课程内容体系，改革教育培训模式，创新教育训练方式方法，以尽快适应新型军事指挥人才的素质能力培养要求。任职型院校要全方位拓展与作战部队联合培养、与外军任职院校合作培养新型军事指挥人才的新途径，适时创新和更新课程内容，加强和完善教学课程内容体系，使院校教学更加贴近实际、贴近实战，走开加速培养新型指挥人才的新路子。

3.3 加快变革培养培训模式

在系统总结近年来探索实践经验的基础上，要进一步围绕未来信息化战争对新型指挥人才的素质能力要求，努力在教育培训模式上实现新突破，走开加速培养新型指挥人才的路子。一是深化复合型培训。以原有专业培训为基础，把院校课堂与军事

行动、部队重大演习活动结合起来,进一步加强对指挥员的信息技术、信息作战和信息指挥素质能力补训。二是加强交叉型培训。以团以上军政指挥员为重点,加强诸军兵种院校之间的交叉轮训和到部队的交叉代职培训,巩固和深化探索实践成果。三是拓展开放型培训。应乘国家经济实力迅速增长和国际地位不断提升的有利时机,充分利用出国考察、进修、留学以及与外军联合演习、参与联合国维和行动等时机,拓展与外军交流的渠道,加速培养具有国际战略眼光的新型军事指挥人才。四是推进实案化的一体化联合训练。以快速发展的一体化信息系统为依托,将分布于陆海空天的各种预警探测系统、指挥控制系统、武器打击系统和支援保障系统深度整合融合起来,有力有效地推进指挥员一体化联合作战指挥训练。这是培养新型军事指挥人才的理想模式,也是今后努力发展的方向。要坚持建、训、管同步发展,尽快形成具有我军特色的新型指挥人才一体化联合训练体制。

### 3.4 加紧信息化平台环境建设

信息化条件下的新型军事指挥人才,必须依托信息化平台和环境来培养。这一方面,我军虽然还很落后,但美军的探索实践给了我们很多借鉴和启示。我们必须加大投入,积极探索创新,尽快取得重大突破。在完善模拟沉浸式训练环境上,大力推进运用计算机模拟仿真技术,建设模拟仿真式生存环境,引人入胜地引导指挥员进行模拟沉浸式训

练,培养信息化基础素质和能力。在完善虚拟现实式训练平台上,大力推进运用灵境理论和虚拟现实技术,建设虚拟仿真式训练平台,进行作战平台与作战环境合成训练,培养指挥员在信息化战场环境中的分析判断能力和对多种复杂因素的坚毅决策与实时指挥能力。在完善分布交互式训练平台上,大力推进运用计算机网络分布技术,建设交互式一体化训练体系,使网络内所有受训的指挥员,都能异地同步地实施联合作战指挥,提升一体化联合作战指挥的本领。

### 3.5 加强政策措施配套改革

新型军事指挥人才培养的紧迫需求,要求我们必须加强政策措施配套改革。要完善具有强制性的培训选送政策,确保将基本素质优良、具有创新精神和发展潜力的指挥军官选送到院校培训,特别要将年轻有为的指挥员苗子纳入精英培养战略工程,实现超前培养。要配套改革培训选升政策,将信息化素质能力作为选拔提升的必备条件,确保经过信息化培训、具有信息化素质能力和工作实绩的指挥军官得到重用,走上重要岗位,发挥领军作用。要结合部队建设模式改革,以“试验部队”为平台,探索“试验部队”指挥员培训轮训制度。要建立健全军事指挥员素质能力测评体系和综合评估数据库,积极探索考核考试选升的新办法,形成科学化、信息化、法制化的管理机制,为新型军事指挥人才成长创造有利条件。

### 参考文献

- [1] 陆春炎,张煜.军事人才思想通论[M].北京:蓝天出版社,2004.11.
- [2] 陈岸然.联合作战亟需人才的素质培养[M].北京:蓝天出版社,2005.7.
- [3] 刘志生.外军军官能力建设概况.北京:解放军出版社,2005.12.
- [4] 叶忠海.人才学基本原理[M].北京:蓝天出版社,2005.3.
- [5] 戴维民.人才管理信息论[M].北京:蓝天出版社,2005.3.

### 作者联系方式

通信地址:武汉市解放公园路45号通信指挥学院发展战略研究所  
 邮政编码:430010  
 联系电话:027-85968235 13329733115

# 以模拟训练为切入点推进一体化训练深入开展

曹光华 洪宇

**摘 要：**一体化训练是适应一体化作战需要的全新训练模式。在目前现有信息技术条件不能完全满足一体化训练需求的情况下，以模拟训练为切入点推进一体化训练深入开展，对于提高部队一体化作战能力有着重要的现实意义。本文分析了模拟训练的特点，阐述了模拟训练在一体化训练中的作用和地位，并就如何科学合理地运用模拟训练以推进一体化训练的深入开展做了一定的探讨。

**关键词：**模拟训练；一体化训练

## 1 正确分析模拟训练特点，开拓组织一体化训练途径

“仗怎么打，兵就怎么练”是军事训练的基本指导思想。模拟训练运用模拟器材或模拟系统，在模仿实战环境下开展的军事训练，它以其显著的训练效果，高效的军事资源利用率，在当今世界军事领域中得到了充分的肯定。模拟训练用模拟的方法改变训练的过程和方式，不仅是对现有训练方式的改革创新，也是组织一体化训练的有效途径，具有诸多新的特点和优势。

### 1.1 近似实战，前瞻性强

模拟训练仿真性很强，模拟的效果几乎与实兵实装一样，使受训者如同身临其境，实战感强，较好地体现了“仗怎么打，兵就怎么练”的思想。良好的模拟训练系统能够利用计算机生成的虚拟作战环境，使受训人员进入逼真的作战环境中进行训练。同时，也可以模拟与战时相同的信息化武器装备，对武器系统、信息系统、人员素质和指挥艺术进行一体化检验，直接为一体化作战服务。因此，以模拟训练为切入点组织开展一体化训练，可以始终瞄准打赢一体化作战的目标，积极借鉴外军一体化建设与训练先进经验，将一体化作战理论研究最新成果应用于训练，不断地设计、创新一体化作战新的作战思想及战法，具有较强的前瞻性。

### 1.2 反应实时，针对性强

先进的模拟训练，一般都借助于计算机技术、图形处理技术、网络技术、软件技术、多媒体技术、现代通信技术、战场监视技术等，以图、文、声、像等多种形式同时或交替切换，或以激光、电子技术，实时动态地反映作战时的真实情况，较好地克服了其他训练方法难以解决的提供情况不及时、处理情况不果断、战法研究空对空、训练针对性不强等问题。因此，以模拟训练为切入点组织开展一体化训练，可以根据任务的不同而创造出不同的近似于一体化作战环境，探索一体化作战的特点和规律，研究不同作战环境下的一体化作战，能更好地提高部队一体化作战能力，具有较强的针对性。

### 1.3 形式灵活，广泛性强

模拟训练能够根据训练需要，改变作战对象、编制装备、地形或改变指挥协同关系、上级决心、友邻行动状态等，适时提供不同训练场景，进行多科目及多种情况的训练。同时，模拟训练可广泛运用于一体化训练的方方面面。在训练对象上，既可以是单个士兵，也可以是一个战术兵团甚至战役军团；在训练层次上，既可以是战术级别，也可以是战略战役级别。因此，模拟训练可根据现有资源灵活组网，进行高层次和大规模的一体化训练，而不必大量集中实兵实装，也可以是模拟单件的信息化武器装备进行操作训练，具有较强的广泛性。

## 2 充分认识模拟训练作用，不断创新一体化训练实践

随着信息化武器装备不断发展，训练模式、方法和手段发生了一定的变化，而在一体化训练中起重要作用的模拟训练的发展却相对滞后，这必将影响到军队的跨越式发展和一体化作战能力的形成。因此，必须要充分认识模拟训练在深入开展一体化训练中的作用和地位，广泛开展模拟训练，对于不断创新一体化训练实践有着重要的意义。

### 2.1 探索未知领域，创新一体化作战理论

一体化训练与作战是一场涉物理域、信息域和认知域的军事革命，有着很多新鲜的、未知的事物需要探索与实践。以模拟训练为切入点开展一体化训练，可以摆脱传统思维观念的束缚，不受现有的武器装备技术条件限制，将研究探索的触角延伸到一体化作战各个领域、各个层次，从而能深刻认识一体化的本质，掌握其特点和规律。在此基础上，在一体化训练实践中不断创新一体化作战理论，去科学构想一体化作战是“什么样”，具有哪些作战样式、作战特点等，预测作战对手作战思想及武器装备的发展趋势，善于从各种现象和因素的发展变化及其相互联系中认识规律，从而形成指导一体化作战和一体化训练的新理论，使创新的理论真正成为启动一体化训练的强大引擎。

### 2.2 理清训练思路，推动部队一体化建设

以模拟训练为切入点开展一体化训练，可以解决条件不成熟训不了的问题，以积极的、理性跨越的方式，科学地、超前地对一体化作战条件或环境进行模拟，通过一定规则和条件参数建立一体化作战模型，模拟出敌我在陆、海、空、天、电不同维度、不同情况下的部队行动，并通过信息化网络控制系统提供适时的各种信息，为受训者提供近似实战的一体化训练环境，从而能使受训者贴近实战去研究一体化作战，在近似实战的一体化训练环境中，充分认清目前军事建设与一体化作战需求之间的差距，从而能进一步理清一体化建设的思路，有利于与部队的一体化建设形成良性互动和提供有益的参照，更好地指导一体化作战理论研究、一体化信息系统建设、一体化作战力量建设和适应一体化作战的高素质人才培养。

## 2.3 超前培养人才，提高一体化训练效益

模拟训练可以部队进行一体化作战训练提供了一定的环境和条件，能使组织者和受训者提前进入一体化作战的演练，通过训练，可以强化信息制胜的观念，认识一体化作战的特点、规律，探索和研究相应的对策，得到近似于实战的锻炼，有效提高指挥一体化作战和组织一体化建设的能力，超前培养和锻炼了一体化作战和建设人才。同时，走投入少、效益高的练兵路子是部队建设的客观需要，由于模拟化训练装备、器材可反复使用，进行模拟训练可避免实兵、实装训练时人力、物力的大量消耗，大大节约作战和训练资源，以最小的消耗取得最佳的训练效益，模拟训练顺应勤俭练兵的要求，在目前武器装备信息技术条件较差的情况下，有效地提高训练经费的使用效益。

## 3 科学开展模拟训练运用，有效提高一体化作战能力

当代高技术特别是以计算机为核心的高新技术蓬勃发展，为模拟训练提供了坚实的物质基础，具备了以模拟训练切入点开展组织一体化训练的条件，模拟训练是否发挥出应有的作用，直接影响一体化训练目的和效果的达成。因此，必须着眼未来一体化作战的特点和要求，加大模拟训练力度，科学开展模拟训练，使其真正能有效提高部队的一体化作战能力。

### 3.1 建立健全模拟训练体系，适应训练需要

模拟训练可广泛运用于一体化训练的方方面面，要模拟训练在推动一体化训练发展上真正起作用，必须适应各级、各类人员训练的多种层次模拟训练体系，使模拟训练能够真正覆盖一体化训练的各个角落。一是模拟训练方法要趋于标准化。为了实现一体化作战的目的，各军兵种的模拟训练在保留各自必要的特殊训练方法之外，必须将模拟训练方法趋向标准化，特别是要在模拟训练系统的建设上加强协作，按照统一制定的标准，向集成化方向发展，实现不同形式的模拟器材、不同种类的仿真系统同地和异地的互联，形成一个大型的作战模拟网络，实施一体化训练。二是建立模拟训练的分层体系。模拟训练作为现代军事训练的一种方式，在

一体化训练中覆盖的训练对象极其广泛,必须区别不同级别的训练对象,建立相应的模拟训练体系。如根据训练对象级别的不同,应相应建立战略、战役和战术层次的模拟训练体系。三是建立模拟训练的分级体系。模拟训练的受训者水平各不相同,并且随着训练的不断深入,受训者的水平也将不断提高。模拟训练也有一个由浅入深、从初级到高级的循序渐进过程,这就需要针对不同训练水平的受训者设定不同难度、不同层次和不同目的的训练科目,构成完备的分级训练体系,以适应不同训练水平及不同受训者的需要。只有如此,才能使模拟训练在一体化训练的全过程中发挥作用。

### 3.2 遵循军事训练客观规律,循序逐级集成

提高以联合部队为重点的作战体系对抗能力是一体化训练的根本目的,体系集成训练也必然成为训练的主线。模拟训练作为训练方法的创新与发展,必然要遵循军事训练的发展规律,坚持由低到高、由易到难、由点到面、循序渐进,按照技能集成、单元集成、要素集成、系统集成,一个环节一个环节、一个层次一个层次地进行,最终实现一体化作战体系的模拟集成。一是进行模拟仿真系统的技能集成训练。模拟仿真系统的技能性训练是开展模拟集成训练的基础。开展模拟集成训练时,应根据模拟集成训练的需求,有计划、有步骤地抓好模拟仿真训练系统的操作技能训练。单兵主要进行装备模拟仿真系统的操作训练,首长机关应加强一体化信息系统的操作训练,并实现各模拟训练系统的互联互通,使各类人员熟练地掌握模拟训练系统的操作使用,奠定模拟集成训练技能基础。二是进行分系统模拟集成训练。围绕提高各作战单元在一体化作战条件下情报信息、指挥控制、火力打击、全维综合保障等作战能力,组织情报信息模拟训练系统、指挥控制模拟训练系统、火力打击模拟训练系统、全维防护模拟训练系统、综合保障模拟训练系统的分类模拟集成训练,突出各作战单元的兵种专业分队在不同战术层次上的分系统合练,实现各作战单元的分系统模拟集成。三是进行综合模拟集成训练。以提高一体化作战能力为着眼点,对一体化

参考文献(略)

作者联系方式

通信地址:合肥市电子工程学院训练部 邮政编码:230037

作战体系进行高度融合,通过相应领导机构组织进行综合模拟集成训练,通过指挥员及其机关的总体设计,围绕统一的作战任务和使命课题,以诸军兵种的信息传输、信息对抗、信息控制为主线,进行高度融合的综合模拟集成训练,实现综合模拟集成训练。

### 3.3 紧密结合其他训练方式,搞好实战转化

模拟训练虽然涉及到一体化训练各个领域和各个层次,发挥的作用与其他训练方式和手段不能替代的。但是模拟仿真毕竟与现实需要存在较大的差距,在深入开展一体化训练中,不能以模拟训练完全取代其他训练方式,而应与其他训练方式和手段相互紧密结合,并做好向实战转化。一是充分认清模拟训练与实装实兵训练的关系。模拟训练与实装实兵训练是现代军事训练的两种不同训练方式,它们之间既相对独立,又相互联系,构成相对完整的现代军事训练模式。相对于实装实兵训练,模拟训练能够形象具体地仿拟复杂、抽象的内容,增强训练效果,减少武器装备的磨损和物资消耗并能保证昼夜间全天候、重复进行训练等等;相对于模拟训练,实装实兵训练也有其无法取代的一面,特别是在训练指战员的实际作战技能以及处理突发意外情况方面有其独特的优势。二是搞好与其他训练方式的结合。在一体化训练中必须应时应地、应科目的需要合理地安排模拟训练的时间比重,使之趋于合理化,并将模拟训练与其他训练方式紧密结合起来。可将模拟训练作为实装实兵训练的前一个阶段,通过模拟训练为实装实兵训练打下坚实的基础,也可以将模拟训练与其他训练方式交替使用或综合使用各种训练方式,充分发挥各种不同训练方式的优长,不断促进一体化训练高效、深入地开展。三是及时向实战化方向转化。以模拟训练的方式开展一体化训练与其他训练方式和手段的最大区别,在于它可以“改变”或“超越”现实,不断地设计、试验一体化作战以适应未来作战的需要。但随着条件的改善,要积极进行实践探索,将模拟训练研究探索的成果不断应用于一体化作战的实践,逐步变虚为实,由训练模拟化向实战化方向转化。

联系电话:0551-5766151

# 顺应空军战斗力生成模式的转变加快空军信息化人才的培养步伐

程建

**摘 要：**本文从空军由机械化战斗力生成模式向信息化战斗力生成模式转变的要求出发，着眼空军院校信息化的发展需要，探讨了加快空军信息化人才培养的思路与对策，提出了优化空军信息化人才培养的学科专业体系、改革信息化人才培养的教学内容、创新信息化人才培养的方法手段等建议。最后探讨了为部队军事训练提供智力与技术支持的方式方法。

**关键词：**战斗力；生成模式；转变；信息化人才

## 1 绪言

人才是推动空军由机械化战斗力生成模式向信息化战斗力生成模式转变的关键。院校必须站在空军“模式转变”的历史高度，构建适应“模式转变”的空军院校教育训练人才培养体系，努力发挥人才培养的主渠道作用、军事理论研究的智囊作用和新武器装备研究的方面军作用，加快教育训练的整体转变，实现院校教育训练的实战化、科学化、正规化和信息化。

## 2 空军战斗力生成模式转变对院校提出了更新更高的要求

随着空军大量的新机、新装备配发部队，空军信息系统建设步伐明显加快，空军信息化程度快速提高，在这由机械化战斗力生成模式向信息化战斗力生成模式转变的关键时刻，对空军各类人才信息化的要求不断提高，从而对院校教育训练提供了难得的发展机遇，也提出了严峻挑战。

### 2.1 空军战斗力生成模式转变要求院校必须加快信息化人才培养

信息化时代的军事人才与机械化时代相比，有着本质的区别。信息化人才的主要特征是：掌握信息化知识和技术，具有信息化思维，熟悉信息化武器装备，能有效利用信息资源，进行信息化建设、遂行信息化作战。信息化人才主要包括指挥人才、参谋人才、专业技术人才等。空军信息化人才是空军战斗力的核心组成部分，是空军转型建设的关

键，空军转型建设要求信息化人才必须把握空军信息化建设与信息化战争的特点规律，熟练掌握空军信息化武器装备的战术技术性能，熟练运用信息化武器装备和军事综合信息系统，实现人与武器装备的最佳结合，组织实施复杂电磁环境下的军事训练和作战行动。

### 2.2 空军战斗力生成模式转变要求院校必须提供强有力的智力支持

院校要按照建设信息化军队、打赢信息化战争的要求改革教育训练，逐步实现教育训练的信息化。推进空军战斗力生成模式转变，就是要通过进一步向信息化聚焦，真正使信息技术成为提高教育训练质量的新的增长点，把战斗力生成模式切实转到依靠信息技术的进步上来，提高空军信息化条件下的实战能力。空军教育训练将在训练内容、训练方法手段和训练组织管理等方面向信息化转变，突出复杂电磁环境下的训练，突出体系战斗力的形成，突出官兵综合素质的提高，在深、精上下功夫见成效，这就要求院校充分利用学科专业密集、人才力量雄厚、信息资源丰富等优势，发挥人才培养的基地作用、军事理论和科技创新的源泉作用、先进战斗力的支撑作用，向部队提供信息化人才和强有力的智力支持。

### 2.3 院校教育训练改革必须适应空军战斗力生成模式转变的需要

院校是人才培养的主渠道。院校教育训练水平，直接影响空军信息化人才的质量，影响空军战斗力生成模式转变的进程。当前，院校建设处于转



轨的关键时期,学科专业体系、教学内容体系、教学方法体系、教学保障体系将发生重大变革。因此,院校必须适应空军战斗力生成模式转变的需要,加快教学改革步伐,建立新的适应信息化人才培养的教学体系,走出一条院校与部队“双向驱动、协调发展”的新路子。

### 3 加快空军信息化人才培养的思路与对策

空军信息化人才的培养必须突破传统的思维模式,强化作战牵引、信息主导、综合集成的观念,坚持“教为战、训为战、研为战”,以学习信息化知识、培养信息化素养、掌握信息化技能、熟悉信息化装备的组织运用和信息化战争的组织指挥为重点,聚焦信息化内容,整合信息资源,创新教育训练方法手段,采取超常措施,加大改革力度,提高训练效益。

#### 3.1 优化空军信息化人才培养的学科专业体系

学科专业是院校人才培养的基础,学科专业的建设水平直接影响着人才培养质量。必须大力加快发展信息类学科专业,运用信息技术对传统学科专业进行改造,以适应空军战斗力生成模式转变对信息化人才的培养需要。

##### 3.1.1 加强电子信息类学科专业建设

把预警探测、情报侦察、通信导航、指挥信息系统、精确制导、电子对抗、综合电子战、网络战等学科专业作为主导专业,加大投入,加快建设,优先发展,使之成为空军信息化人才培养的主要依托。

##### 3.1.2 利用信息技术对传统学科进行改造

加强信息技术向作战指挥、航空工程、导弹工程、机械工程等学科领域的渗透、交叉与融合,拓宽专业内涵,增设专业方向,突出对目标探测、识别、对抗和对新装备武器的研究,加大学科专业梯队、实验(习)室等软硬条件建设,提升学科群的整体发展水平,使传统学科的优势更加明显。

#### 3.1.3 创建与新技术、新装备发展相适应的新兴学科专业

着眼天基信息资源下的空天一体作战需求,积极培育天基平台信息系统学科专业,逐步形成新的研究方向和专业教学能力。

### 3.2 改革信息化人才培养的教学内容

教学内容直接决定着人才的知识、能力和素质结构。按照空军战斗力生成模式转变对各类人才的要求,调整人才培养目标,以信息应用技术牵引教学内容改革,突出基础性、加强综合性、强化针对性、增强创新性。

#### 3.2.1 着眼信息素质培养,加强信息知识教学

根据各类人才培养目标,用信息化的要求、信息化武器装备的发展和信息化战争的理论改革传统的课程体系,加强信息技术、网络技术特别是信息获取、信息传输、信息处理、信息运用、信息攻击与防护等方面的教学内容,提高人才的信息科学素质。其中,生长干部学员要突出信息化知识、军事信息技术及应用等教学内容;研究生学员要突出信息检索、信息处理、信息攻击与防护等教学内容;任职教育要把信息系统系统集成、一体化训练、最新信息技术等作为教学内容。

#### 3.2.2 贴近空军信息化建设,增加信息战教学内容

按照空天一体化、空军信息作战和空军武器系统综合发展的要求,增加航空航天技术、信息集成技术、空军新武器系统概论和战场电磁频谱管控、信息作战指挥等课程,重点加强指挥信息系统、通信网络系统、信息侦察与监视等教学,使各类专业教学内容体现信息化特色。

#### 3.2.3 贴近空军作战,突出信息化技术和装备教学

着眼空军信息化作战,加强情报获取、指挥控制、快速机动、综合打击、多维防护和整体保障能力的培养,以适应高技术条件下信息作战的特点和要求。加大实战背景特别突出复杂电磁环境下的训练;注重系统与系统、体系与体系之间的对抗性训练,将战术、技术、指挥与管理融为一体,使教学内容与部队装备发展相同步或超前。

### 3.3 创新信息化人才培养的方法手段

#### 3.3.1 以新装备教学为重点,积极探索模拟化训练方式

把模拟训练作为大型武器装备和复杂专业训练的重要步骤。依托模拟仿真实验室和各类训练模拟器,改革训练方法,改进训练素质,使院校训练逐步走开计算机虚拟、模拟系统仿真、实装训练、综合演练“四步训练法”的路子,做到模拟苦练、实装精练,真正使学员理论上学懂弄通,操作上会干会用,胜任岗位。

#### 3.3.2 以信息资源利用为重点,积极推开网络化训练

把运用现代化网络技术作为教育训练的重要手段,积极开展网上训练和教学。依托全军军事综合信息网、校园网等信息资源,将校内和校外各种训练系统、模拟系统甚至实际装备进行联网,进行想定作业、技能研练、网上推演、网上对抗等训练。在训练中,设置“蓝军”,模拟作战对手的特点,进行对抗性训练,增强院校教育训练的针对性和实战性。

#### 3.3.3 突出复杂电磁环境,探索基地化训练的路子

把基地训练作为提高信息化条件整体作战能力的重要方式。依托院校综合性训练基地和部队实践基地,营造贴近部队、贴近实战的训练环境,按照部队岗位设置角色,进行融战术、技术于一体的训练。特别是要设置复杂电磁环境条件,突出电子侦察、电子进攻、电子防御技术训练和战法研练。

### 3.4 完善信息化人才培养的保障条件

#### 3.4.1 创设网络化的教学环境

网络化教学是信息化教学的显著特点,可以共享资源,增强教学效果,实现教学的合作互动,有效地促进学员实践、创新能力的提高。一是构筑信息化的网络平台,二是大力开发应用网络资源,三是积极开展网络教学。

#### 3.4.2 加快新装备现地教学的基地化

基地化教学是增强教学针对性,提高学员驾驭新装备能力的有效途径。专业化的训练基地建设,

必须充分运用现代信息技术,与武器装备系统有机结合,构成体现信息化战争特点和要求的现代化教学环境。一是在院校建立综合训练基地,二是抓紧建设适应信息战要求和高层次人才培养的网络战、综合电子战和 C<sup>4</sup>ISR 关键技术实验室等,三是加大向院校配发新装备的力度,四是在部队建立新装备现地训练基地。

#### 3.4.3 加强教员专业能力的培养

坚持教员任职资格制度,所有承担任职教育任务的教员必须有相应的部队任职经历。下大力提高教员的专业教学能力,采取到部队调研、代职见习、参加重大演习活动等措施,使教员熟悉部队、熟悉新装备、熟悉作战训练保障。积极选调具有实践经验的部队优秀干部到院校,从事指挥专业和装备使用维护课程的教学工作。

## 4 为推进空军战斗力生成模式转变提供智力与技术支持

院校应适应空军转型建设需要,主动置身于空军战斗力生成模式转变之中,在创新军事理论、生成作战能力、检验训法成果上发挥能动作用,为部队训练提供强有力的智力与技术支持。

### 4.1 为空军部队军事训练提供理论支持

院校应贴近部队、贴近实战、贴近任务,着眼信息化条件下空军军事训练的特点和规律,开展重大现实理论问题研究。一是复杂电磁环境下军事训练研究。重点研究模拟未来战争的复杂电磁环境设置、作战指挥、装备运用、技术保障等方式方法和特点规律,梳理总结训法战法,为部队训练提供依据。二是加强空军信息化建设问题研究。重点研究空军信息化理论体系、空军信息化建设、外军信息化的发展等课题,积极开展空军信息化发展需求论证,指导部队信息化作战、训练的实践活动;三是为部队训练提供信息咨询。编写信息化知识普及系列丛书,参与编修条令法规和新装备操作规范。针对新装备使用中存在的问题进行对策性研究,为部队提供情报信息支持。

## 4.2 为空军部队军事训练提供技术服务

围绕军事训练转变中的重难点问题,创新训练方法和手段,为部队军事训练提供技术咨询和技术支援。一是提供模拟仿真训练环境。利用院校实验室进行装备模拟系统的开发、训练平台的搭建、战法的模拟验证,开展信息对抗训练等;二是进行技术保障。根据各种装备的使用性能和特点,组成技术保障分队、建立新装备技术保障数据库、开展远程教学和故障诊断等,协助部队搞好装备训练。三是到部队进行信息化知识培训。抽调专家定期到部队开办信息化知识培训班,普及信息化知识。四是加强院校科研成果向部队训练的转化。在院校建立军事理论和科技成果转化平台,推进科研成果向军事训练转化,提高训练效益。

## 4.3 为部队演习演练提供智力支援

部队的演习演练是和平时检验信息化人才培养质量和部队训练质量最直接有效的形式,对院校教育训练和部队军事训练都具有十分重要的作用。一是参与部队训练、演习方案的制定。组织院校教员与部队指挥员合力攻关,在训练程序、方法、手段和内容上,谋求运用信息化手段整合训练、演习资源,提升训练、演习质量和效益;二是参与部队训练、演习的组织与行动。与部队指挥员通力合作,针对演练过程,战场态势发展,及时调整预案,锻炼部队在复杂情况下的应变能力,特别是在复杂电磁环境中,催生一批新训法、战法,推进部队训练、演习向更高层次发展;三是参与部队训练、演习的效能评估。组织院校教员,参与部队重大训练、演习活动的评估,寻找训练、演习中存在的问题,提出解决的思路与方法,不断提高部队训练、演习的水平。

## 参考文献

- [1] 刘联华主编.《信息化军事大视野》.北京:海潮科学出版社,2007年3月
- [2] 刘海主编.《军校信息素质教育研究》.北京:军事科学出版社,2006年12月
- [3] 张蜀平主编.《直面信息化战争》.北京:国防工业出版社,2007年1月
- [4] 商则连主编.《国防和军队信息化建设理论研究》.北京:军事谊文出版社,2006年5月

## 作者联系方式

通信地址:西安市沣镐路东1号176分号

邮政编码:710077

联系电话:029-84799304

# 信息化战场建设与人才问题研究

丁武将 杨雪南 胡思远

**摘 要：**本文从信息化战场的建设角度，探索性地研究了国防与军队信息化人才队伍建设的几个基本概念和实际问题。提出了信息技术基础工业自主创新能力的提升，是当前信息化战场建设应当高度重视的关键点。信息化战场建设中的军民结合、两用技术和军民一体化，不仅涉及到人才的发现、培养和使用问题，而且是未来战争中全面有效地运用信息力量的基本问题。

**关键词：**信息化战场；信息化人才；军事力量运用；信息技术基础工业；两用技术

## 1 信息化战场建设需要高度重视体系对抗能力的提高

刚刚结束伊拉克战争的美国人，首先做的第一件事不是去发展他的飞机大炮，而还是进一步构建自己的信息战场。美国的国防部长亲自上阵，以构建“战争互联网”为起点，让美军指挥官和部队利用所谓战场上的“上帝之眼”，实时获得战场上敌我的动态信息，不仅使美军拥有比对手更快速更大范围调动作战资源，比对手更快更精准地发挥火力的能力，甚至还可以通过信息对抗（阻止、截获、篡改、伪造等）等手段，直接影响对手的判断与决策，巧妙调动对手的行动与部署，继而利用对手的火力与资源。可以这样认为，美军的信息化战场已经从电磁空间构建在了全球他们认为可能“构成威胁”的国家。更为重要的是，他们的信息化战场，还通过计算机软件、芯片、标准、网络等技术的引领性，通过市场与经济的方式，悄悄地构建到了那些没有足够防范的同样是他们认为可能“构成威胁”的国家。

从西周置烽燧以来，我国有过古代“立国重边，威震八方”的辉煌历史，也有近代百年“有边无防，任人宰割”的惨痛教训。人们常常把国防与战备、与军队等同起来，把国防仅仅看作是军事领域内的事，是军队的事，把视野局限于“守疆界，护版图，筑篱笆，砌长城”。然而当今世界风云变幻的教训一再告诉我们，对国家安全的威胁不仅仅来自军事的威慑和战争，它往往在军事行动之前，早已在政治、经济、科技、文化、体系对抗能力（战场建设）等诸多方面打下“胜兵先胜而后求战”的基础。无论是“内陆型国防观”、“海洋型国防

观”，还是“高边疆国防观”，其实都是不同历史阶段对国家安全防务的狭隘理解。这种对国防观念狭窄的、片面的认识和理解，就是所谓的“小国防”观念。

除了观念上的问题以外，还有判定上的问题。国防与军队信息化顶层设计，必须建立在对一些大的问题的判断基础之上，才能使“设计”不会出现大的偏差。比如，判定威胁、判定战争、判定战场、判定敌人、判定敌人的作战方式和基本作战体系、判定敌人的基本武器装备体系和基本走向等等。其中，构建具有体系对抗能力的信息化战场，是顶层设计不可回避的重大问题之一。

设计与构建信息化战场的体系对抗能力，必须针对特定的对抗者与其相应的体系，有的放矢，有针对性地去建设，否则空泛的、无的放矢的、靠大量资金“引进”技术与设备堆积起来的体系，很可能在严酷的战场对抗中只是一堆垃圾，甚至成为对手攻击己方所利用的工具，这就是所谓“双刃剑”效应。

然而，世界风云变幻莫测，未来的“战场”在哪里难以判定，“战场”上究竟是什么样的对手，也同样难以准确推测，继而，“战场”上的对手所使用的作战方式，更是扑朔迷离。如果将一个国家的电力信息系统、电信信息系统、金融信息系统等等战略性的系统体系纳入国防的概念里面，那么，面对这样的由许许多多无形系统或有形网络组成的“战场”，其定数就更少，其防范就更难。如何做好顶层设计，构建具有体系对抗能力的信息化战场，必然进入两难境地。

然而，如果从构建信息化战场的能力体系上入手，兼顾可能的威胁，就有可能走出两难，摆

脱困境。而且,将构建信息化战场的能力体系作为切入点或着力点,更容易找准高技术或引领性创新技术的切入点,是贯彻落实军民结合这类高层次国家战略体系的有效途径,也是继承和发扬新时期的“人民战争”这一光辉思想的有效措施,是将国防与科技、经济有机地结合起来的成功发展模式。

那么,构建信息化战场的能力体系包括什么内容呢?我们现实已经出现的威胁又是什么呢?我们已经进入了战略经济的时代,经济已经成为国家战略的主要命脉。经济的本质动力,来源于技术创新和引领。自主创新精神已经成为一个民族的战斗精神!其中,信息技术创新与引领能力的建设,将成为信息化战场建设的根本保证!围绕信息技术创新与引领能力的建设,构成了信息化战场能力体系建设的主要内容。因为在那里,有太多的战场,有太多的未来军事工业基础,有太多的军事潜能。

我们已经出现的威胁,是没有硝烟的市场大战,是那种通过不断技术创新和引领,逐渐占领和摧毁你信息产业能力和诸多主要产业能力的市场大战。因为我们非常清楚,未来的军事潜能很大程度上将取决于一个国家的信息能力,特别是信息产业的能力。而信息产业能力的本质,是产业自主创新能力和国家组织运作能力在市场大战中获得认可的程度。

事实上,信息化战场的建设,在很大程度上取决于信息技术创新与引领能力的建设。

信息时代的战争与机械时代的战争最大的不同,就是战争的打击目标发生了根本性的变化。机械时期的战争,平时是进行扩军备战,战时专门攻击战争潜力。而信息时代的战争,平时是占领你的信息工业基础,瓦解你的军事电子工业,战时就专门攻击你的信息目标。

军火巨头洛克希德-马丁公司首席执行官说,他预见军事和情报活动融为一体的高度安全互联网将主宰 21 世纪的战争。就像核武器的出现左右了整个冷战时期的军事思维。届时每一名军人都能获得整个战场态势的感知能力,好像拥有“上帝之眼”。已开始组建战争网络的国防情报安全局战略计划主任称:“网络中心战的实质就是使美军具有在任何时候向任何地点部署作战部队的的能力,而信息技术是达到这一目的的关键。”

这是我们没有经历过的新型战场!我军过去长于地面作战,对现代信息战和空袭反空袭作战经验

不多,对于构建这样的战场能力,更是缺乏经验。未来我与敌人在信息战场上的较量,将更多集中在平时的战场能力建设和争夺上,这种能力上的竞争或争夺,将可能成为具有决定意义的较量。

我们习惯了守卫传统意义上的“地理疆域”,而对于“电磁边疆、网络边疆”的守卫,已经成为不能回避的历史重任。然而,设计并打造守卫这种无形边疆的能力,或者,设计并打造这种无形战场的能力体系,不仅仅是军事人员或国防科技与工业人员的职责,而必然成为我全国人们尤其是信息科技工作者负有的神圣职责。构建我们的现代化的信息化战场能力体系,是我国全体人们所面临的历史性的挑战!!

## 2 信息化战场的建设者也是信息力量运用的人才队伍

如果说我们的武器装备与主要大国有巨大差距,我们的士兵训练与素质也有差距等等,这些都不是主要问题。我军的辉煌历史一再证明了这一点。何况,在当今全球一体化的浪潮下,除非内部出现重大问题,否则技术与装备出现过大的代差的可能性越来越小,即使个别技术与装备出现较大的代差,然而整个技术与装备体系却不会被拉得太远。因为就整个大的体系而言,跟进模仿终归比自主创新要容易一些。反过来说,如果连跟进模仿都会被拉下过大的代差,那么可能出现的战争中,“武器装备体系”在战争胜负问题上的发言权就可能需要军事专家们重新论证了。当然,一味跟进模仿,虽然整个体系不会出现过大代差,体系的效用值不差,但却有对抗性不高的风险。

关键问题是,我们的信息化战场顶层设计,却不能与主要大国出现历史性的距离!

恩格斯所说,“一旦技术上的进步可以用于军事目的,并且已经用于军事目的,它们便立刻几乎强制地,而且往往是违反指挥官的意志而引起作战方式上的改变甚至变革。”

军事革命对军队建设、战场建设提出了新的挑战,也对军事人才提出了全新的要求。我们必须造就出高素质的、平时能构建能力体系的、战时能驾驭和指挥未来高技术信息战争能力的各类人才群体。

适应信息时代的需要和军事革命的挑战,我军

事人才观念，尤其是培养和造就高层甚至顶层军事人才观念，必须有一个大的提高。此外，军事人才的群体结构，也必须不断地进行调整。而当务之急的是，必须有效地组织和造就顶层设计人才队伍。信息化战场体系能力的建设，关键来自顶层设计的预见性、谋略性、对抗性和各种技术运用的先进性。更为重要的是，在未来有形战场与无形战场有效结合的复杂战场环境下，必然会出现的事实是，信息化战场的建设者将是军事力量运用的关键人员。

简单的事实可以说明，在软件和芯片成为装备的今天，软件与芯片的设计与开发人员最清楚自己的软件或芯片的“漏洞”，一旦对手使用这样的软件或芯片，同样也最清楚该如何破坏、如何攻击、如何置入病毒、如何使其系统崩溃。我们看过无数技术高手运用技术有效打击对手的“大片”，其素材当然来自越来越多的事实。

在信息技术高速发展的今天，信息化战场的创造者，很大程度上将不能仅仅或过多地依赖军事部门和军事人员，军事部门和军事人员将更多地关注构建信息化战场能力的需求，关注如何创造具有体系对抗能力的战场，关注如何有效地运用未来构建出来的信息化战场，而将大量的具有很大风险的探索性、创造性的工作，留给广大的科技部门和敢于技术创新的企业部门，在这片土地上，有太多的军民两用，有太多的原始创新。也就是说，我们必须学会区分体系设计与运用的帅才将才，还要学会区分体系设计与建造的帅才将才。毕竟，设计、建造、运用，是完全不用的概念，但是却有许多交叉的部分，需要有机地结合，才能发挥总体优势。

当然，我们还要区分运用人才与运行人员。运用者主要确定作战运用的方向、方式方法（或战法）、以及运用的力量体系，有效地综合运用各种资源，获取战场优势，夺取战争胜利，他们实际是未来战场上的指挥人员。而运行人员，是按照指挥人员的要求，有效地运行职责范围各类信息化装备，他们实际是士兵，确保整个作战体系的顽存和有效运行，所谓人在阵地在的概念。当然，我们必须清楚地意识到，战场信息流程中的每一个士兵，不再是传统战争中担负几乎相同任务的单独作战单位，而是整个战场信息链中的一部份。这就是“十人一杆枪，百人一辆车，千人一枚弹”的形象比喻。今天，如果要发射一枚战略导弹，从确立目标

到测量目标，直到编制程序、装定诸元、发射控制、命中目标，这一系列的作战行动中，如果哪一个环节、哪一个人出了问题、都将导致‘兵熊熊一窝’的悲剧发生，整个作战行动可能彻底失败。

我军在长期的革命战争和建设过程中，造就了一代又一代优秀军事人才，积累了丰富的经验，形成了优良的传统，走出了一条成功的道路。今后一个时期内，我军的信息武器装备仍将处于劣势，在这种情况下，要战胜对手，就要发扬优良传统，把坚定正确的政治方向放在首位，坚持人民战争和人民战争的战略战术，不仅要继续坚持任人唯贤的军事人才路线和德才兼备的人才标准，而且还必须继续坚持从信息化战场建设的实践中造就与培养人才各类人才，包括军事力量运用人才的务实观念。

### 3 通过军民结合自主创新提高我信息化战场的体系对抗能力

我们有过军转民的历史，也同样尝试过民技军用的艰难。但是新的时期，军民结合军民两用体系下的自主创新，却是我们无法回避的历史性挑战，前苏联的教训让我们认识到高度重视军民结合是国防与经济协调发展这一国家战略。纵观世界各主要国家，尽管信息化武器装备所需要的信息技术，70%~80%来自民用技术，只有20%~30%来自军用技术，但军用技术却发挥了引领性作用。军用技术从高风险的引领性创新提高，到技术向民用市场的溢出，再到民技军用，实现通用的货价产品，这些都显现了历史规律：1991年以前，原创信息技术启动，大都来自军方，随后技术溢出，转化民用；1991年至2003年前后，逐渐形成军民一体化的融合体系，“民技军用”是再转化的自然结果；2003年至2006年以来，商用现货不能满足国防需要，再一次开始了以国防技术引领发展的关键性驱动。

军队信息化、信息化战场建设都与一个国家的信息技术能力经密不可分。当前，信息技术领域出现了以下“融合”趋势：技术创新与产品联系密切；产品与市场密不可分；信息安全与信息产业紧密关联，信息产业与军队信息化息息相关，军民结合的军事电子工业与信息化战场建设息息相关。所谓战略经济，显著的特征就是，国家战略将越来越多地通过行业战略和企业战略来实现。

我们将面对的信息化战场，是由强大的信息技术、产业、商业等等所支撑的整体对抗体系，在这样的战场上，“战争”不仅表现在有硝烟的战场，在平时更多地表现为没有硝烟的战场拼杀：科技强大发达的国家，平时就在挖空心事进行人才掠夺、资源掠夺、产权掠夺、磁场与空间掠夺，其表现出来的“市场大战”早已刀光剑影，你死我活。信息技术遥遥领先的发达国家，牢牢掌握并控制着信息技术与体系的制高点，通过技术渗透等方式，不仅彻底动摇你的信息技术工业基础，而且使你整个作战应用所建立起来的信息技术体系和架构都“不出如来佛的掌心”。表面上你实现了现代化和信息化，而实际上无非构建了一个受人控制的“空中楼台”。

“兵者，诡道也”，诡道者，不守常也。“不守常”的实质是“变”，能因敌变化而取胜者谓之神。“变”的关键在于最大限度的保持弹性、韧性和灵敏性，保持高效的快速反应能力。“变”的核心是“奇正”。善战者，以正合，以奇胜。在信息时代，体系对抗的内涵将不断丰富，“用奇”，不仅表现为技术与装备的不断推陈出新，“杀手锏”装备层出不穷，不仅表现为能因敌变化而创造并有效实施出克敌制胜的作战方式方法，还表现为平时的信息化军队建设中，通过给对手各种误导，甚至通过信息技术的渗透和货架产品的商业供货，早就埋下伏笔，打下了“胜兵先胜”的基础。难怪美国前总统克林顿强调：“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”可以说，一个国家支配信息资源的能力越强，就越有战略主动权，而一旦丧失了对信息的控制权和保护权，就很难把握自己的命运，就没有国家主权可言。

这不能不引发我们注意到：信息化战场建设，不可以缺少战场建设的能力体系和人才，更不可以缺少顶层设计组织与人才，而未来的战争中，这两种人员，都将是战场的杀手，他们与军事需求和作战运用人才一起，都是未来军事力量体系当中的重要人才。然而，这两种人才，是在信息化战场的建设中造就出来的，是设计与建设的艰难过程中自然形成的。

此外，我们必须意识到：信息化战场的顶层设

计需要实践中不断探索螺旋发展。在我们平时鼓足干劲“建功”的过程中，我们不能忽视了我们所赖以构建军事能力的军事电子工业，这是完成独立自主的技术体系，是军民结合的自主创新体系。一切引进、跟进、模仿，都是为了创新与发展，还必须为了制约与对抗。正像俄罗斯的基本方针：在广泛收集其他国家先进技术情报的基础上，进行独立研制。他们收集、借鉴的目的在于独立研制，在于制约对手，在于超前对手。

战场上的主动权，需要在军事斗争准备中去寻找；有利于我的非对称作战，需要在军队建设和军事科研中去创造。军队信息化顶层设计的主旋律，依然是为了适应新时期争夺战场主动权来展开的。美军利用其强大而有不断国际领先的信息技术优势，在军队信息化方面长足发展，不断形成新的不对称优势，牢牢占领制高点，把握主动权。此外，他们不仅一直在把握“领先”的主动权，而且还不断地将其他国家引领到他们的体系中，尽可能让他们认为有“威胁”的国家，进入与他们基本类似的体系建设中来，从建设体系上，也同样牢牢把握主动权。事实上，是美国政府和国防部的战略体系，使美国不断地牢牢控制信息技术发展方向，保持了其核心技术的绝对垄断地位。深入研究其机理，有一点值得我们认真反思，那就是其国家层面的高度重视并由国家意志进行精心组织筹划。可以说，美国电子信息产业的发展，始终是国家战略层面极为关键的环节，而且美国国防部在其中起到核心、主导作用。在其国家信息产业发展战略的整个体系中，从框架、目标、实施步骤及对关键环节的控制（如因特网开放协议等），完全是由国防部组织筹划确定的；其战略实施中的关键技术突破（如网络所用多种器件的研制攻关等），也是由国防部大力经费支持当前我信息化战场建设顶层设计的关键点，不是花费大量经费购买“现代化”和“信息化”，而是必须脚踏实地，从基础军事电子做起，解决战略性、关键性的基础技术，彻底摆脱基础平台和技术体系完全跟进的框框，走出一条独立自主的道路，只有这样，才能在未来的体系对抗中，从顶层设计开始就牢牢打下“立于不败”的战略基础。

## 参考文献（略）

## 作者联系方式

通信地址：北京丰台区大成路 13 号院 18 号楼 54 号 邮政编码：100039 联系电话：010-66820824

# 信息化条件下炮兵旅级单位通信建设的几点思考

都迎东 崔星

**摘 要：**通信是炮兵信息化武器系统的重要组成部分。通信分系统，作为指挥自动化系统的组成之一，正起着连接信息获取系统、信息处理系统、组织指挥系统、火力控制等系统的重任。在这样的条件下，通信系统的保障问题就成了现代条件下战争保障中必须关注的关键问题。要想在现代战场上不受制于人，就必须充分分析现代高技术局部战争的特点和通信建设的规律，立足现有条件，努力寻求提高我通信系统综合保障能力的有效途径，在一旦面临高技术局部战争时能有所准备、有所对策，不致丧失战场上的主动权。

**关键词：**通信；建设；信息化

随着我军现代化、信息化建设的逐步深入，在编制体制上出现了更多的旅级作战单位，如何有效提供安全稳定的通信保障，是现在面临的新的挑战。如果从编制上进行一些调整，特别是在旅直属连队之中建立直属通信连，将进一步加强通信保障的能力，尽快实现通信兵的军事训练转型，将加强旅级作战单位在应对未来信息化条件下的局部战争的总体作战水平。

## 1 旅级单位通信保障现状及存在的问题

### （1）通信分队与其他各专业混编保障

我军现有编制的大部分旅级作战单位多为兵种分队，在编制上通信分队是与其他各专业分队混编在直属的两个指挥连，指挥连不仅是要保障通信联络而且还负责指挥、侦察等各方面的保障任务。保障任务重，内容多，从通信联络保障的角度看保障的有效性不高，效果不是很好。

### （2）通信训练组织难

通信分队编制于指挥连，相同的专业又分属于两个不同的连队。在组织专业训练时只能以排为单位进行训练，甚至以班为单位进行。训练过程中通信部门检查指导难，训练的标准不高，两个直属指挥连之间同专业协同训练少，给战时通信保障带来了一定的影响。如无线专业在战时或演习时综合组网后，各电台之间相互不熟悉，容易给敌台的窃听和干扰提供可乘之机。

### （3）通信部门与通信分队指挥协调难

由于直属指挥连队保障的内容多，在进行通信

保障时通信部门下发的通信指示多是直接交由排长和班长进行执行。通信部门组织保障将直接面对战士。对每条线路，每个节点都必须进行实际的安排。通信部门工作量大，指挥难度大。而通信部门直接安排和指挥通信保障人员也容易引起与连队安排相冲突，影响保障工作。

### （4）通信专业人才培养难

目前的通信部队编制对于保留通信专业人才造成了一定的影响，通信学兵学习回来后不一定就能安排在其所学专业上，使学习机会白白浪费。对于一些专业好，技术精的士官由于编制问题无法保留，连队的主官既要会指挥专业又要掌握通信专业，部分通信出身的军官由于专业受限不得不改学其他专业，使大量的通信人才流失。这些情况使通信专业上形成了人才严重缺乏，甚至出现断代现象。

在信息化条件下实现通信兵训练转型是一项长期的工作，我个人觉得应遵循以下几点：

## 2 战时运用多样化，提高通信对抗能力

### （1）实现训练转型，提高训练水平

以炮兵部队为例，作为重要的火力单位，在未来战场中将发挥重要的作用，通信分队是炮兵实施有效火力保障的重要力量，是敌方重点打击的目标，我们要着眼于未来信息化条件下的战争特性，不断实现炮兵通信兵向信息化训练转型。

### （2）着眼实战，提高训练要求

未来战场环境恶劣，对通信兵的要求更高，我们要着眼于实战需要出发，利用驻训等机会强化通



信兵在高寒山地特殊条件下的进行通信保障能力,提高训练的质量和标准,以适应未来战场的需要。

### (3) 动静结合,以通为主

无线电通信,容易被敌人侦听、测向和干扰。但在具体实施中,若注意隐蔽和伪装,是能够减少和避免的。保持无线电静默便是其中一法。所以,在炮兵作战中,无线电通信既要做好隐蔽和伪装,又要做好保障作战指挥。也就是要做到“动”,“静”结合。怎样才能达到上述要求呢?一是提高认识,克服胆怯心理。在电子战中,敌对双方都是以各种电子侦察手段来截获,破译对方的内容的,但这种侦察和破译是需要时间的,就是最先进的设备,测得一个电磁波辐射方向也大约需要 15 秒钟,采取快速通信的方法,就完全可以避开敌人侦察。二是“静”中有“动”,相互结合。在部队作战中,以无线电静默来隐蔽其企图是必要的,但绝不能影响其作战指挥的中断。因此,在炮兵无线电通信中应做到“动”中有“静”,“静”中有“动”。既隐蔽自己又保证部队的作战指挥。三是以“动”掩“静”,实施无线电静默可以起到隐蔽自己的目的,但是完全靠静隐是不够的,既要“静”、又要“动”,必要时可以“动”掩“静”。现代战争中虽然侦听、测向技术有了很大提高,但是只要精心组织,周密计划,是可以达到隐蔽自己,迷惑敌人的。

### (4) 隐真示假,虚实并用

隐真示假,就是利用电子伪装,响动等电子欺骗手段,对炮兵作战企图、部署和行动进行隐蔽,以形成有利于我方战役态势的一种电子对抗战法。在隐真示假中常利用无线电佯动来实施。所谓无线电佯动,是指利用无线电运动通信来模拟部队的机动。炮兵通信在实施佯动时,通常是在作战的次要方向突然增加无线电装备的数量和联络对象,或启用一定规模的通信网、实施无线电佯动,模拟较大规模部队行动。这样既可转移敌人侦查重心,又可以大大减小我主要作战方向的通信抗干扰压力。

### (5) 宁小勿大,扬长避短

宁小勿大,扬长避短是炮兵无线电通信反侦察的一项有效措施。所谓宁小勿大,就是在使用电台时,能够在小功率未通时,不用大功率;能用小功率电台的,不用大功率电台。因此,在组网和选用电台的时候,应注意把握。采用上述措施,能较好地控制信号的传输距离,使敌人难以侦收我方无线

电信号。所谓扬短避长,就是在选用电台的时候,能用短天线通的,不用长天线;在通信的时候,尽量发短报或短话。电台所装备的天线有多种,且不同的天线其通话距离是不同的。使用时应正确使用,切不可为了追求信号的强度而用长不用短。信号在空中暴露的时间越长就越容易被敌人捕捉到,我们发信号的时候要尽量压缩内容,要严格遵守上述条件。

## 3 优化编制,建立旅直属通信分队,提高通信保障能力

在不改变现有旅级作战单位两个直属指挥连的前提下,将两个直属指挥连整合成一个通信连,一个指挥连,可以进一步优化我军在旅级作战单位的编制,既可以提高其他各指挥专业的协同作战能力,更可以有效提高旅级作战单位的通信保障能力。

### (1) 有利于加强通信保障的可靠性

建立直属通信连后,通信力量更为集中,人员、装备都能集中于一个连队,在实施通信保障过程中便于调配,通信部门的通信指示可由通信连来组织落实,通信连可根据连队实际情况提出有效可行的实施方案。避免了通信部门对连队人员、装备情况不熟悉造成的指挥失误。也避免了连队在保障过程中面对机关有多个业务指导部门工作头绪过多的情况,加强了在战时和演习等重大活动中通信保障的可靠性。

### (2) 便于统一组织通信训练,尽快实现通信兵军事训练转型

通信分队集中编制后,通信连可以统一组织各专业的军事训练,强化专业之间的协调性。连队能真实地掌握各专业的训练水平和保障能力,及时地对训练中存在的问题进行纠正,对训练中暴露出来的薄弱环节可以进行整改和调整完善。使过去训练不好搞、搞不好的问题得到解决。在训练过程中,连队能结合自身实际,按照上级的计划和安排进行信息化条件下的各类训练,从现实出发加快军事训练转型的步伐,能有效提高通信分队的训练质量。

### (3) 有效提高通信部门对通信分队的指导作用

通信部门在进行检查指导通信训练、值班、基础设施建设上也有了很强的针对性,通信部门能集中进行检查,特别是连队能及时上报相关的信息,

出现问题能及时得到解决，克服了通信部门下去摸不准脉，通信分队的问题又上报难的情况。在向信息化条件下军事训练转型过程中训练必然面临许多新的问题和困难，及时有效地解决好这些问题对推动通信兵的军事训练转型有着很大的促进作用。

#### （4）增强通信人才培养的持续性和有效性

建立直属通信连后，可以选配通信专业对口的军官任职，使通信军官在实践中提高自身水平，加强指挥通信分队进行保障和计划组织保障的能力，也避免了由于编制上的限制使通信军官流失的问

题。在选送通信学兵时，连队能根据日常掌握的信息选送专业技术好，素质过硬的战士进行学习，毕业学兵直接安排进入通信连，连队也能根据学兵素质和连队实际情况合理安排。连队中专业、技术精的士官可充分发挥作用，不断培养和训练新战士，使通信人才的培养不间断，能形成一个合理的良性循环机制，把人才变为一种“软件资源”，人走人才不会走。为通信分队确实保留好一支珍贵的人才力量。

### 参考文献

- [1] 林象平.《电子对抗原理》.北京：国防工业出版社，1981年
- [2] 《中国军事百科全书电子对抗和军用雷达分册》，1993年
- [3] 王稚.隐身技术.《现代军事》，1987年
- [4] 袁宗福.《炮兵通信战术》.1994年

### 作者联系方式

通信地址：云南省昆明市金碧路 77200 部队 13 分队

邮政编码：650032

联系电话：0871-4770303 13888619001

# 信息化战争条件下军校如何推进现代化教学改革

刘晓宁 宋绯 邓莉

**摘 要:** 本文首先论述了军队院校实行现代化教学改革的必要性,而后从适应军事变革需求和军队建设人才需求两个方面阐述了如何推进适应信息化战争的教学改革,本文的最后提出了适应信息化战争教学改革中应注意的四个问题。

**关键词:** 信息化; 教学改革; 军事变革

## 1 实行现代化教学改革的必要性

世界格局如今正在发生重大变化,单极世界已对国际社会稳定造成严重威胁。伊拉克战争充分说明,未来的高技术战争,无论是战争的规模、形式、以及陆、海、空军在战争中的作用、地位都与传统战争发生了截然不同的变化,战争重心已向信息化转移。

20 世纪 90 年代以来,以新技术特别是信息技术的发展为动因,科学技术的迅猛发展,引发了军事领域的又一次深刻变革,形成了军事理论研究的第四次高峰。当今的战争转型使军事斗争呈现出新的特点,军事理论、战争形态、作战样式的变化,对人才培养提出了新的更高的要求,也给我军建设特别是军校教学改革提出了严峻的课题。

### 1.1 战争转型期内在矛盾的特殊性促使军校教学改革

战争转型是非突变式的质变。机械化战争的破坏力以核武器的出现作为极限的标志。而由机械化战争向信息化战争的转型则是系统化的推进。研究当代战争系统推进的内在矛盾的特殊性,是加强军校教学改革的首选。

当前战争转型期,主要的目标是提高打击精确度,实行“精确制导”。精确度的提高对战斗力起到倍增作用。信息战使得民用信息技术介入战争成为可能,使得原本是非战争因素的社会力量直接介入战争成为可能,从而使战争从另一面增加了很多变数,面临失控的危险。研究信息战条件下诸多内部矛盾的特殊性,有助于把握战争的走向,把握新时期军事斗争的特殊性,从而为军校教学改革发挥

先导作用。

### 1.2 新军事革命促使军校教学改革

信息战是一个不可逆转的时代潮流。各国的军队建设不能不考虑到这个潮流。但是如果盲目地去“紧跟”这个潮流,又容易导致与自身实际情况相脱节。因此,寻找我军的定位,寻找军校教学改革的定位,就有一个把时代潮流与自身实际相结合的问题。

在这种情况下,一方面,应当绝对和相对地加大军费投入,集中优势加强信息类院校的建设;另一方面,力求在存在“时代差”的非平衡态中寻求自己的优势,使我们的信息战能力具有中国特色。要充分估计到我们仍有很多自己的优势,有自己的“杀手锏”。更何况近几年我们在信息战、电子战能力建设方面发展较快。美国航天部负责人埃伯哈特说,中国日益发展的电子战能力让美国越来越依靠网络的作战受到很大威胁,他们很担忧。

新技术革命呼唤着哲学的革命,呼唤着方法论的革命。而面对军事变革中高技术的应用,面对战争转型期出现的诸如电子空间、网络空间等各种复杂的新事物,军事哲学的发展显得很贫困。没有军事哲学的变革,没有军事认识方法论的变革,对很多问题的认识只能是“雾里看花”。从这个意义上讲,军事哲学的变革是战争转型期技术变革深层次矛盾的抽象折射,对指导新时期军队建设具有深远的意义。无疑,军事哲学的变革是军校教学改革——尤其是军事理论类院校教学改革的重头戏。

面对新形势,应及时调整我军发展战略方针,推进新的战略性转变,应对世界军事变革的挑战,谋划国防发展的良策,在未来的高技术战争中立于不败之地,适时推进中国特色的军事变革。军校是

培养军事人才的摇篮,军校只有加快教学改革步伐,才能适应高素质新型军事人才培养的迫切需要。加速推进现代化教学,提高人才培养质量,也是当前和今后一个时期院校教育改革和发展的主题。因此,军校要推进现代化教学,积极探索现代化教学的思路,树立好现代化教学的理念,以指导军校的教学活动。

## 2 怎样推进适应信息化战争的教学改革

### 2.1 推进军校教学改革以适应军事变革需要

#### 2.1.1 必须从整体上对教学内容进行系统定位,采取相应的改革措施

新的历史时期,有的学科已整体上不适应军事斗争的需要,应予以淘汰;有的学科则是部分不适应,或深度、广度上不适应,急需发展;有的领域则需要开创新的学科。进行系统定位是全局性的,应当由总部组织专家统筹规划为主,各院校自我论证为辅。在此基础上才有可能进行学科的有机重组,进行人力、物力、财力等教育资源的有机重组,适应新时期军事斗争的需要。各院校科研项目的立项和实施也应全军一盘棋,避免重复研究。

#### 2.1.2 切实加强院校与部队、与外军以技术、教学骨干为主的多层次交流

有的院校虽然是搞信息战的,但是教员自觉地深入部队的很少,对外军信息战资料掌握得也很少。这样显然不能适应战争转型、军事斗争准备的需要。实践证明,在加强院校与部队的交流方面,还应以全军统筹安排为主。近年来,海军在这方面作了些尝试,取得了一定的效果。主要的方式就是将部队和院校的技术、政工干部交流岗位,为期半年。但是存在两个问题有待改进:一是交流的层次不高;二是影响范围窄,效果不明显。

#### 2.1.3 军校素质教育应以适应战争转型为龙头

具体讲,可从三个层面入手。一是理念层面,即促使学员在学习中逐步树立起要将自身的学习与战争转型的特点有机结合的理念;二是知识层面,即给学员传授与军事斗争准备需要相适应的知识;三是能力层面,即培养学员现代指挥、科学研究等

多方面的综合能力。这三个层面是相互联系、相辅相成的。院校可在以课堂教学为主阵地的基础上,通过请专家学者讲学、组织学员下部队实习、组织学员参与科研项目等措施,培养出适应战争转型期军事斗争需要的复合型的高技术军事人才。

### 2.2 推动军校教学改革以适应军队建设人才的需求

#### 2.2.1 从学员实际情况出发,树立“以学为中心”的育人观

在传统的教学模式中注重强调教员的主导地位,而忽视了学员的主体地位。现代化教学要求我们对传统的教学指导思想进行调整,从过去的教为中心转变为以学为中心。教员在教学中的传统角色要发生变化,不仅仅是知识的传授者,还应该以指导者、组织者、研究者、学习者的身份参与到教学中,激发学员学习的主动性和积极性。对学员学习的要求,不仅是“学会”,更重要的是“会学”,是“学会学习”。要把教员唱“独角戏”,变为师生互动式的“二人转”,要由一般性的、分散性的知识传授,变为专题式的、系统性的问题研究。以学员自主学习,自我发展、自我完善为目标,科学设置自修内容,为学员提供自主学习空间。要加大实践性教学环节,通过加大实践教学时间与内容的比重,加速学员所学知识向能力的转化,实现人才的德、智、军、体全面发展。

#### 2.2.2 更新观念,营造现代化教学氛围

“均衡发展”的观念与现代化人才培养所需要的“群体合格,个体突出,全面合格,特长突出”的非均衡人才培养观念之间的矛盾;灌输式、填鸭式的传统教学观念与培养学员能力和提高素质为目标的启发式、研究式教学观念之间的矛盾;更新观念就是要从传统教育观念中脱壳。这个“壳”是受传统教育体制决定的整套传统思想观念,解决这个问题,应从四个方面入手:第一要牢固确立教育观念现代化的意识。第二是要增强人才培养的责任意识。第三要注重在教学实践中转变观念。要营造现代化的教学氛围,要形成现代化教学气息,创造现代化教学环境。第四要注重现代教育技术与传统教育媒体的结合。现代化教学方式多元化的特征,使得多种教学组织形式相互结合成为可能,教育者在教学组织形式上可以根据学员各自的特点实施个性

化教学。

### 2.2.3 在教学手段上, 树立科学运用的实效观

在教学过程中, 不能单纯的只重视提供外部刺激, 让学员机械地、重复地适应外部的刺激, 忽视对学员对外部刺激的信息加工过程的研究和指导, 忽视对学员的构建知识结构的指导。在使用多媒体进行教学时, 我们不能陷入“唯多媒体教学论”的误区, 应注重将传统教学媒体(如幻灯片、录音机、电视机、挂图等)和现代教育技术手段相结合, 适宜用什么就用什么, 从而发挥最大的作用。教员要处理好教员、学员、媒体三者的关系, 让教员的主导作用贯穿于教学过程的始终。

### 2.2.4 深化教学改革, 努力提高教学质量

教学既然是“教”和“学”的有机结合, 那么教学改革就不仅仅是教法的改革。军队院校的教学质量, 在一定程度上确实取决于教材内容与部队生活、社会生活的接轨。所谓教学, 某种意义上就是通过教材启发受教育者思考一门课程的各种问题, 进而创造性的提出问题, 解决问题。首先选择合适的教学模式教学方法艺术地教学, 才可能提高学员的素质。二要是使学科内容结构化, 通过让学员掌握各学科的基本概念、原理和法则, 达到触类旁通, 举一反三的效果。三是要使课程设置综合化。打破学科界限, 加强学科联系, 开设综合课程, 打破单一的课程结构, 设置多种类型的课程。

## 3 适应信息化战争的教学改革应该注意的几个问题

当然, 在推进军校教学改革的时候, 我们不能只注重改革, 忽略一些很重要的问题, 这样也许会产生不必要的麻烦, 适得其反。因此, 我们应妥善处理以下几个关系。

### 3.1 妥善处理坚持继承与创新发展的关系

继承和创新都是推进时代发展的巨大动力。没有继承, 创新就是无源之本; 没有创新, 继承就是因循守旧。开创工作的新局面, 必须坚持创新, 但创新要有连续性, 不是割断历史, 院校教学中已被实践证明是行之有效的东西必须保留, 继续发扬光

大。同时, 根据国防和军队建设以及文化教育事业发展的新目标、新要求, 用新的思路和新的举措, 确保教学工作在继承的基础上不断创新发展。根据时代的发展, 部队装备的更新换代, 高科技的普遍推广, 适时修改、完善各种教学规章制度、教材, 更新教学手段。

### 3.2 妥善处理基础教育和军事教育的关系

军校教育作为国民教育的重要组成部分, 决定了军事人才的培养既要适应高等教育的基本要求, 又要具有鲜明的军事特色。军队院校的教学工作必须积极响应党的号召, 为实现党的教育方针和奋斗目标做出贡献。这种贡献是通过培养大批高素质新型军事人才, 达到国防和军队建设的战略目标来实现的。因此, 我们在推进现代化教学的过程中, 要充分借鉴国家高等教育的成功经验, 坚持高等教育的质量规格, 达到国家高等教育的基本水准。军校毕业的学员, 应具有地方高等学校同等学历学生的基础知识, 符合教育部的人才培养目标。同时, 要着眼“打得赢、不变质”的根本要求, 突出培养目标的强制性、人才岗位的职业性和教育形式的规范性, 培养出“政治合格、军事过硬、作风优良、纪律严明、保障有力”的合格军事人才, 真正走出一条有我军特色的教学路子。

### 3.3 妥善处理遵循程序和超常跨越的关系

事物的发展都有一定的程序过程, 这是事物的常态。但在特定的历史阶段, 可以打破常规。军校工作, 应按照“发展要有新思路, 改革要有新突破, 开放要有新局面, 各项工作要有新举措”的要求, 以实施现代化教学工程为契机, 不断创新思想观念、不断创新人才培养模式。使军校教育主动适应军队现代化跨越式发展的需要。同时, 也要坚持从实际出发, 把革命精神和科学态度结合起来, 避免违背客观规律、违背科学、盲目蛮干。

### 3.4 妥善处理当前工作和长远建设的关系

贯彻好军校教学改革的重要思想, 必须做到既对历史负责又对当前负责。从长远讲, 就是要按照江泽民同志国防和军队建设思想以及建设“五支隊伍”的总要求, 大力实施人才战略工程, 为我军现代化建设提供强有力的人才支持。当前, 在教学工

作指导上,要以解决现实问题为中心,以提高教学质量为重点。把主要精力放在抓落实、打基础上,扎扎实实地做好日常性教学工作。按照这一思路,我们应全面实施军队院校现代化教学工程,持续抓好教学质量检查,逐步完善科学的教学工作评价体系,引导院校进一步深化教学改革。加快素质教

育、创新教育、力争在不长的时间内构建起各级、各类人才新的知识、能力和素质结构体系,实现教学内容、方法、手段、管理改革的整体突破,使人才培养的数量和质量进一步适应军队现代化建设和军事斗争准备的需要,为我军院校的长远建设和发展奠定坚实的基础。

### 参考文献

- [1] 刘中路等.论信息作战指挥的影响及对策.科技信息,2007年第4期
- [2] 梅梅等.“院校的建立、人才的培养”至关重要.黑龙江科技信息,2007年第5期;1卷
- [3] 黄书科.从速度、精度和跨度看信息化战争.现代防御技术,2007年第2期;35卷
- [4] 朱丽华.军校现代化改革的第一要务.南京政治学院学报

### 作者联系方式

通信地址:南京市御道街标营2号通信工程学院9信箱

邮政编码:210007

联系电话:025-80828117

# 复杂训练仿真系统研究

何彬 王禹淇 王琦

**摘 要：**训练仿真系统在我军训练体系信息化建设中发挥着越来越重要的作用。本文探讨了复杂训练仿真系统的理论基础，如：训练仿真系统的作用、特点，并从系统分析和能力分析两方面对笔者的研究进行了阐述。最后展望了训练仿真系统的发展方向。

**关键词：**训练仿真系统；系统分析；能力分析；发展方向

作为军事仿真系统的一种，训练仿真系统能够根据作战训练的要求，为参训人员提供类似于实战的训练环境。其优点在于可以突破地形、气候的限制、减少实兵演习的次数，提高演习的规模，增强演习的真实程度，有效地降低训练的开支，提高训练的质量。另外，通过网上模拟演习，还可以避开军种兵种或其他体制壁垒，在网上营造虚拟战场空间，加大联合作战训练的力度。在我军训练体系信息化建设中，训练仿真系统发挥着重要作用。

在当前实际开发的训练仿真系统中存在着如下问题。

当前的训练仿真系统多为简单系统，设计的训练层次和作战实体较少，难以进行较大规模的仿真训练。

当前训练仿真系统的功能不够完善，战场态势显示不够直观。训练过程中，参训人员不能很好的对作战进程进行干预，其意志不能得到充分的体现。

当前训练仿真系统的通用性、扩展性差，导致系统难以适应训练要求的变化。

笔者以某训练仿真系统的开发为背景，对复杂训练仿真系统的设计进行了研究，提出了复杂训练仿真系统的一般设计思路，并对解决上述问题的途径进行了探讨。

训练仿真系统对参训人员可以起到以下几个方面的作用：首先，可以激发思维。训练仿真的最大作用就是激发参与者的思维，而参与者越是深入地参与到作战仿真过程之中，这种作用就越大。

其次，可以促进思考。如果参与者还参与了建立模型，提出了具体目标，选择了决策准则，提出了想定和假定条件，把自己的想法深深地嵌入到了战争模型之中，那就能更深刻地思考，利用仿真系统做出更好的决策或得出更好的结果。

再次，易于分析比较。许多军事训练要求对作战方案进行全面的比较和分析，用以比较各种备选方案。要满足这一要求，可以在可控制的仿真条件下，对多组假定和输入条件进行多次反复地模拟来做到。

第四，易于定量评估和裁决。一些军事训练要求得出具有定量数值的结果，采用具有较准确模型的训练仿真是实现这一要求的唯一方法。

第五，可以积累经验。任何对问题的研究，对武器装备的把握，对指挥及操作技能的熟悉，都需要大量的时间和反复地“试错”。通过训练仿真积累大量的经验，从而也就减少了在实际战争中犯同样的错误的可能性。

## 2 复杂训练仿真系统分析

### 2.1 复杂训练系统的提出

笔者参与开发了一种大型的训练仿真系统，由于该系统可以进行几个不同层次的仿真训练，并且不同层次的系统可以进行交互和协同工作，因此该系统属于复杂训练仿真系统，笔者以该训练仿真系统为例子来探讨复杂训练仿真系统的开发。

## 1 训练仿真系统概述

训练仿真属“人在回路”的虚拟仿真（Virtual Simulation，“真实的人在虚拟的环境中操纵虚拟的系统”的仿真），即“人”作为训练的对象，处于仿真回路中，在仿真系统创造的战场环境中，不断的经受锻炼和接受接近真实的体验。

2.2 复杂训练仿真系统的架构

该复杂训练仿真系统根据作战方案，通过对作战地（空）域范围内的战场态势和敌我双方装备的运行情况进行动态地仿真，利用网络向作战指挥控制系统实时提供模拟的信息数据流，包括下属各系统上报的信息流、上级指挥机关下发的信息流以及友邻的支援情报等，提供类似真实战场指挥所的环境供参训人员训练。该训练仿真系统由从由高到低的 A、B、C 等 3 个级别的训练仿真子系统组成：

A 级训练仿真子系统模拟 A 级（高级）指挥所下属各 B 级部队上报的信息数据流和部队部署信息及运行状态信息和友邻支援的情报。

B 级训练仿真子系统模拟 B 级（中级）指挥所下属各 C 级（低级）部队上报的信息数据流和部队部署信息及运行状态信息，以及 A 级指挥所下发的指令、情报和友邻支援的情报。

C 级训练仿真子系统主要模拟其下属的作战分队上报的信息数据流和部队部署信息及运行状态信息，以及 C 级指挥所下发的指令和情报信息。

3 个级别的子系统均可以根据特定的运行方式，输入特定的实体数据、过程与活动数据、计算模型、指令与报文协议，构造特定的代理程序、用户界面和控制系统内部运行的逻辑。从而实现各自系统训练仿真的目标。

2.3 复杂训练仿真系统的工作方式

该复杂训练仿真系统的工作方式非常灵活，3 个级别的训练仿真子系统可以单独使用，分别支撑相应层次的训练，也可以同时进行不同层次系统的互联。可以实现以下几种工作方式：分别支撑单个

训练子系统的运行；同时支撑两级训练子系统的运行；同时支撑三级训练子系统的运行。在三级训练仿真子系统互联时，要求整个系统内的训练仿真子系统协同运行。

复杂训练仿真系统的运行控制系统主要用于协同不同仿真子系统的运行。其协同内容包括三个方面：第一，各个仿真训练子系统模拟的目标相关；第二，各个仿真训练子系统模拟的作战想定时间相关；第三，保证各个仿真训练子系统同步运行。

2.3.1 支撑单个仿真子系统的运行状态

该训练仿真系统可以支撑各级子系统单独进行训练，这种状态下 3 级训练仿真子系统相互之间是独立的，可以使用不同的想定场景。

2.3.2 支撑两级仿真子系统运行状态

该训练仿真系统可以支撑任意两级训练仿真子系统的运行。在这种情况下，这两级子系统之间能够协同，并且使用同一个想定场景，由运行管理控制系统来协调两级子系统的运行。

2.3.3 同时支撑三级仿真子系统的运行

该训练仿真系统可以同时支撑整个三级作战仿真子系统的同时运行，此时 3 个级别的训练仿真子系统，使用同一想定，同步运行。

3 系统的能力分析

该复杂训练仿真系统的能力包括以下四个方面：想定场景管理、作战装备仿真、作战目标仿真、导调与控制。如图 1 所示：

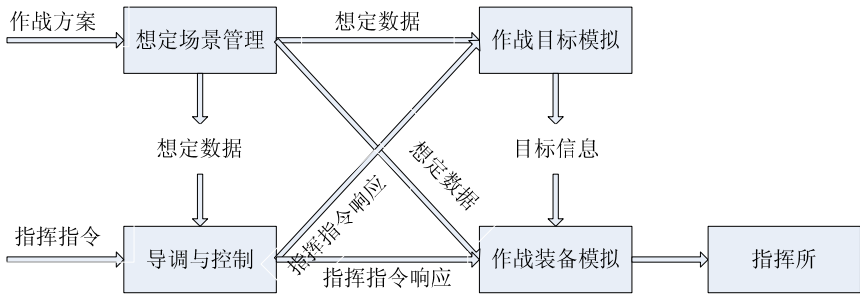


图 1 作战训练仿真系统功能图

3.1 想定场景管理

想定场景管理包括作战计划管理、装备数据管

理、想定管理、想定态势显示四个子模块。

作战计划管理实现对作战计划的管理功能，完成对作战计划数据的存储。



装备数据管理实现对敌我双方装备数据的采集、管理维护。

想定管理显示训练仿真系统中的敌我装备种类、数量、部署、责任区域等信息；设置各个装备的航迹、活动和交互时间，设定作战行动初始条件和结束条件等；确定作战装备工作的参数范围等信息。实现对于想定场景的打开、关闭、存储、复制功能。

想定态势显示能够显示作战想定的态势数据，完成对于敌我双方作战目标的标绘，实现想定数据的基本图上操作功能如部署标绘、航迹设定等。

### 3.2 作战装备仿真

作战装备仿真的功能是：

- a) 模拟作战装备的运行，按指定格式上报装备部署信息、工作状态信息；
- b) 模拟作战装备的侦察和情报综合能力，接收作战目标信息，依据侦察模型，生成侦察情报，按指定格式上报；
- c) 接收系统下发的指令和情报查询信息，并做出响应；
- d) 接受导调与控制子系统的控制信息；
- e) 显示作战装备的感知态势。

### 3.3 作战目标仿真

作战目标仿真的功能是：

- a) 模拟作战目标的运行，公布其性能参数、状态信息；
- b) 模拟作战目标的侦察、探测等能力；
- c) 可以响应导调信息，作战目标受到攻击后要能够做出处置，实现仿真目标对战场态势的响应；
- d) 显示作战目标的感知态势。

### 3.4 导调与控制

导调与控制的功能是：

- a) 控制仿真训练系统的运行；
- b) 保证多个仿真训练系统的协同运行；
- c) 时间管理；
- d) 提供对作战装备和作战目标人工干预能力；
- e) 接收上级提供的实时作战目标数据；

f) 实时显示整个作战想定的客观态势。

## 4 未来发展方向

随着计算机技术和网络技术的不断发展，现今的仿真已经从单武器平台的性能仿真发展到复杂环境下的多武器平台体系对抗仿真，仿真体系经历了从集中式、封闭式到分互式、交互式的发展过程。复杂训练仿真系统的发展方向是能够模拟战术，战役多层次，多兵种协同作战的分布式、可扩展的仿真系统，为了实现这一目标需要采用 HLA、MDA 等技术。

### 4.1 基于HLA的分布式复杂训练仿真系统

HLA (High Level Architecture) 是美国国防部 (DoD) 发布的建模与仿真大纲中，建模和仿真应用技术框架中的首要内容，其主要的目的是促进仿真应用的互操作性和仿真资源的可重用性。基于 HLA 的仿真系统具有许多优点：具有良好的可重用性、互操作性。能提供更大规模的将构造仿真、虚拟仿真、实况仿真集成在一起的综合环境、可以建立不同层次和不同粒度的对象模型等。

虽然 HLA 具有良好的可重用性、互操作性等特点，但 HLA 本身只是一个框架性的规范，只为仿真组件的重用和互操作提供了基础，但没有给系统实现提供具体的技术方案。与一些常用的建模技术，例如 UML 语言，没有建立直接的联系。因此仅仅基于 HLA 体系来设计复杂分布式的可扩展的训练仿真系统是不够的，还需要采用 MDA 架构的模型体系来增强仿真系统的通用性。

### 4.2 应用MDA的可扩展仿真系统

应用模型驱动体系 (Model Driven Architectonics, 以下简称 MDA) 的仿真系统是一种利用通用的模型，在统一的仿真框架内根据需要，将通用模型具体化为特定领域的模型并运行，以达到仿真目标的仿真系统。其关注的焦点是使仿真系统在功能上有更强的扩展性，在性能上有更好的伸缩性。

在基于 HLA 的训练仿真系统中应用 MDA 具有以下优点。

- 1) 标准会随着时间不断成熟和发展，MDA 提

供的机制，可以有效地保障仿真模型适应不断变化的仿真标准，友好地进行模型的转化和演进。

2) 采用 MDA，使 H LA 与现有的软件体系结构标准和发展相一致，扩展了 H LA 的应用范围。

3) 应用 MDA，模型成为仿真的设计关键，它将促进各类仿真人员更好地沟通，更重要的是由于最终平台实现是集成考虑的，这样行为建模可以不受过多因素的干扰。

## 5 结束语

本文介绍了笔者对于复杂训练仿真系统的认识，着重探讨了复杂训练仿真系统的开发思路，提出了自己的设计方案，并展望了这类系统的发展方向，可做为类似复杂训练仿真系统开发的参考。但是由于专业知识的局限，当前建立的系统在细节方面还需要进一步的完善，有待继续研究。

### 参考文献

- [1] 孙岩.面向服务的作战指挥训练仿真系统体系结构研究[D].北京: 装甲兵工程学院, 2006.3
- [2] 王琦, 孙岩, 何彬.基于模型驱动体系的方案分析型仿真系统建模[J].装甲兵工程学院学报 2007.6
- [3] 柏晓莉, 柏晓辉, 李恒峰, 罗雪山. 基于模型驱动体系的 HLA 建模仿真研究[J].计算机仿真 2007.6
- [4] Anneke Kleppe, Jos Warmer, Wim Bast 解析 MDA[M].北京: 人民邮电出版社, 2004.

### 作者联系方式

通信地址: 北京装甲兵工程学院信息工程系

邮政编码: 100072

联系电话: 010-66719314 13269221966

# 信息化军事人才培养方式探讨

洪宇 孙冲

**摘 要:** 随着科学技术的快速发展及在军事上广泛应用, 培养一大批适应未来信息化战争需要的信息化军事人才, 成为目前推进我军信息化建设最紧迫的问题之一。本文着眼于未来信息化战争的需求, 提出了信息化军事人才培养的基本方式, 分析人才培养的主要途径, 并对提高人才培养质量的方法进行了探讨。

**关键词:** 信息化; 军事人才; 培养方式

随着科学技术的快速发展及在军事上广泛应用, 在未来信息化战争中, 信息化武器装备将会大量运用, 使战争成为智能的较量, 学识的交锋。没有一大批高素质新型军事人才, 就无法掌握先进的信息化武器装备, 无法创造和运用新的战法, 就不可能赢得战争的胜利。因此, 研究和探讨信息化军事人才的培养方式, 加快培养出形成部队战斗力急需的信息化军事人才, 对于发挥信息化武器装备的最大作战效能、提高部队的作战能力、推动我军现代化的跨越式发展有着极其重要的意义。

## 1 院校教育、实践锻炼、自我发展相结合是培养信息化军事人才的基本方式

院校教育具有系统性、规范性、专业性的特点, 是培养军事人才的主渠道。但是, 军事人才的培养是一项针对性、实践性很强的活动。战法的运用、信息化武器装备的使用、作战行动的组织实施等仅靠院校学习是无法掌握的, 必须在军事实践中才能真正得以学习掌握。同时还要看到, 现代科技发展迅猛, 知识更新速度加快, 必须用自我发展的方式进行弥补。

### 1.1 充分发挥院校教育培养主渠道作用

院校教育, 是军事人才获得系统军事理论、专业技能和组织指挥知识的基本途径。信息化战争的需求对军队院校教育提出了更高的要求, 军队院校必须要利用自身优势, 发挥主渠道的作用。一是要创新人才培养观念。要确立信息主导观念, 突出

人才信息素养的培养, 将信息知识、信息技术和信息战理论渗透到人才培养的全过程、全方位, 构建以信息化为核心的现代教学体系; 要确立系统集成观念, 运用综合集成的方法, 拓宽人才专业面和培养渠道, 建设信息化教学平台, 开展全方位、多领域、多模式育人的实践活动; 要确立能力本位观念, 针对未来信息化战争的需求, 大力加强实践性教学环节, 把能力训练落实到教学的各个环节和各个方面。二是要创设综合化课程。培养信息化军事人才要打破课程设置传统模式, 筛选和优化专业基础课的知识点, 重组分散各门课程间的相关内容, 开设综合化课程, 实现由单一知识点的培养向知识综合化方向转变, 实现单一课程无法实现的效果。三是广泛运用现代化教学手段。在教学中, 要普遍应用多媒体教学手段, 可以加强学员的直观印象, 加深对知识的理解; 要充分利用网络教学平台建设成果, 使学员能自主学习相关知识, 教学之间能自由地进行研讨与交流; 运用计算机模拟手段, 使教学更加灵活直观, 增大信息量, 提高教学效果。

### 1.2 在军事实践中摔打人才

在军事实践中增长才干对于信息化军事人才成长具有特别重要的意义。军事实践既可以使他们自觉地锻炼自己, 获得实际工作经验, 激发进一步学习的欲望, 又能把自己在院校所学的知识与部队建设的实践相结合, 将知识转化为素质, 转化为能力。一是要在机关与基层中滚动锻炼。在基层与机关中滚动任职, 有利于信息化军事人才的全方位积累经验, 增长才干。要有计划安排基层和机关干部进行双向交流, 使对信息化军事人才既是能参善谋的智囊型人才, 又是具有较强指挥作战和组训能力

的指挥员。二是加强专业间岗位轮换。从未来信息化战争的需求来看,要克服片面强调“专业对口”的传统思想,有计划、有重点地安排信息化军事人才在专业岗位间互换任职,将其培养为既是掌握现代科技知识、驾驭高新的武器装备的高层次技术人才,又要培养为精通本职、适应现代信息化战争的优秀指挥员。三是注重利用重大军事活动锻炼人才。部队进行重大军事活动时,要把培养信息化人才作为重点突出出来,采取跟训跟演、观摩见学等形式以练谋略、练指挥、练协同、练技能,并充分发挥信息化军事人才的主观能动性,研究解决遇到作战中的重难点问题,有意识地摔打锻炼人才研究新情况、解决新问题的能力。

### 1.3 用自我发展全面提升素质

信息化军事人才的成长是一个长期学习实践和自我完善的过程,不仅要接受院校教育和实践锻炼,还要充分调动主观能动性,坚持勤奋自学,使自己的知识结构始终处于合理优化的状态,以适应未来信息化战争的需要。一是要学会自主求知。信息化军事人才必须要不断增强自我学习、自我发展的内在动力,使之能根据自身基础和实际需要,选择和采用适于自己的有效学习方式,研究自己迫切需要知道的问题,并善于运用新知识,研究解决新问题,形成新能力。二是与院校教育相统一。院校教育必须以自学为基础和支撑,才能达到良好的效果,信息化军事人才必须把在院校中学到的系统的军事理论和知识,通过自学来消化、吸收、充实和扩展,使知识具有连续性、延展性和实用性。三是与岗位训练相结合。要紧密联系岗位训练实际,以问题作为学习的载体,形成自觉以问题为中心,围绕问题展开学习的知识积累、思考研究、发现创造等活动,实现知识增长点与部队需求点的“对接”,使自己在任职岗位上增长才干、提高能力。

## 2 院校、厂所、部队三位一体是培养信息化军事人才的主要途径

“院校、厂所、部队”三位一体培养信息化军事人才,反映了高层次的军事人才培养规律,有利于发挥“院校、厂所、部队”各自的优势,有利于弥补军队院校培养能力和资源的不足,有利于培养

一批科学文化素质较高、有发展潜力、有较强实战能力的军事人才,从而适应未来信息化战争的需要。

### 2.1 院校与厂所进行联合培养以形成“院所一体,教研一体”的优势

院校与厂所一体化进行人才培养,有利于提高教学、科研的整体效能,促进教学、科研的双向互动,强化战术与技术训练的紧密结合,为培养信息化军事人才拓展了新的方式与途径。一是主动前伸,搞好作战理论研究。作为院校提前介入信息化武器装备的研制中去,尽早展开作战理论研究,把作战理论与信息化武器装备研制有机地结合起来,对其在未来信息化战争中的地位和作用进行的理论论证,以指导研制工作,同时又能掌握信息化武器装备的第一手资料,适应对信息化军事人才培养的需要。二是发挥优势,实现技战术结合。信息化武器装备是建立在复杂的技术基础之上的更高层次的战术。厂所参与培养人才,为技术和战术的有机结合走出了一条新路,能发挥其在技术上的优势,能够使人才更好地掌握信息化武器装备的性能特点、工作原理、操作使用,信息化军事人才在精通技术基础上创新与应用新的战术。

### 2.2 加强院校与部队联合使人才培养贴近前沿、贴近实战

由单纯的院校教育走向院校部队联合培养,符合军事人才成长的客观规律,是军事教育的一条重要原则。院校教育与部队训练联合培养,不仅使部队训练能够及时地吸收院校教研的最新成果,发挥院校的人才资源和信息资源优势,而且能够有效克服院校教育存在的与部队实际脱节的现象,有利于提高院校教育的针对性和有效性。一是要加强组织领导。要着眼未来信息化战争的需要与发展趋势,制定好特色鲜明、针对性强的院校与部队联合培养对信息化军事人才规划,对今后一个时期内院校与部队联合培养的人才进行科学筹划和部署。二是要制定育人互动制度。通过多种渠道、多种形式,安排和协调教研人员到部队实践,参加部队重大演习和训练等任务,同时院校要积极聘请部队领导、优秀骨干授课辅导,将部队作战任务转化为人才培训的具体需求,便于院校有针对性地进行教学。三是建立实践性培养基地。部队和院校相互协调,选择

和建设相对稳定的有关部队和训练基地作为人才培养基地,以积极组织信息化军事人才以指挥员或组织者的身份,参与部队实兵演习和重大训练活动,体验部队作战、训练环境,提高人才指挥作战能力。

### 2.3 按照“优势互补、资源共享”的原则进行部队与厂所共同培养

采取部队与科研厂所相结合的形式,能充分利用双方的资源和信息技术优势,加速信息化军事人才的培养。要针对各部队的不同特点,通过加强知识衔接、优势互补和资源共享,达到合力育人的目的。一是依托厂所培训。部队主动与生产厂家联系,根据需求,选派具有相应人才到生产厂家培训,并通过邀请技术专家来部队讲课,让信息化军事人才及时了解当今最新技术、各种信息化武器装备的现状与发展趋势。二是搞好接装培训。在换装中,请工厂、研究所的科技人员给信息化军事人才系统全面地介绍信息化武器装备的知识与技术,边学习边进行换装实践,要使之尽快地熟悉了解装备的性能特点,掌握使用和管理方法,打牢作战使用的必备理论和技术基础。

## 3 模拟训练、网络训练、基地化训练紧密融合是提高信息化军事人才培养质量的有效方法

以信息技术为核心的高新技术迅猛发展,引发了军事训练手段的更新变革,传统的训练方法手段,已难以满足人才培养的需求。培养信息化军事人才必须着眼未来,树立超前思想,将模拟训练、网络训练及基地化训练融为一体,紧紧围绕作战需求,磨砺信息化军事人才指挥作战的过硬本领,有效提高人才培养质量。

### 3.1 积极创造条件,在模拟训练中提高灵活运用战术能力

模拟训练能在现有条件满足不了信息化军事人才培养需求的情况下,创造一个近似作战的训练环境,使培养的标准、内容和质量能够最大程度地贴近实战要求,同时它也是操练技术、研练战术、研究战法的重要方法与途径。一是进行装备模拟。在

信息化军事人才培养的过程中,对一些信息技术含量高、现在还难以装备部队但又必不可少装备,要确定技术标准,进行技术模拟,从一定程度上解决装备不能满足现实需要的矛盾,确保人才培养质量。二是作战环境模拟。综合运用计算机仿真技术、网络技术、激光技术和数字通信技术等手段,创造近似于实战的训练环境,使受训者在这种环境中接受近于实战的检验,锻炼实战能力。可根据任务的不同而快速创造出不同的作战环境,设置多种危难复杂的局面,以更好地锻炼信息化军事人才在纷繁复杂的局面中快速决策、快速处置的能力。三是决策思维模拟。指立足实际情况,从理论思维上对未来作战环境进行科学构想,前瞻性地探索信息化武器装备作战的特性和趋势,积极探索对策与措施,形成科学的、先进的作战理论与方法,加快进行信息化军事人才的培养。

### 3.2 科学构建系统,在网络训练中增长指挥协同能力

网络训练是军事训练的必然走向。采用仿真手段,在网络提供的虚拟战场环境中,开展网上训练,能更好地实现对抗演练,实现信息化军事人才在异地、远程能同步进行训练,是最贴近实战的训练方法。一是开发网络训练系统。要集中院校、部队、科研单位等多方力量,力争开发瞄准未来作战对手、贴近未来战场环境、具有全维战场景况视觉效果、能提供复杂多变情况的网络训练系统,为提高指挥能力提供良好的训练平台。二是逐级联训提高协同能力。未来作战将是一体化联合作战,必须充分利用网络的链接性、整体性、互动性,加强一体化联合训练。先组织单网单级单训,尔后进行多网多级联训,将全网内不同军兵种,在不同级别、不同单位所进行的同一课题的统一训练,实施全网互动、整体联训,提高信息化军事人才指挥及协同能力。三是强化网上对抗训练。信息化军事人才培养必须紧贴未来信息化战争的实际,采取多种对抗形式,遵循由低到高、分步细训的原则,按照单级单项对抗、单级多项对抗、多级多项整体对抗的递进顺序进行,进行同地室内或异地网上对抗模拟演练,提高信息化军事人才指挥协同能力。

### 3.3 完善基础设施，在基地化训练中砺练人才实战能力

基地化训练是人才培养向高层次发展的必然趋势。要使作战训练真正满足信息化战争条件下的综合化、逼真化、实时化、联合化等要求，就必须实现训练的基地化。一是构建近似实战的战场环境。训练基地建设，应与未来信息化战场相一致，尽可能地提供近似实战的战场环境，提供复杂的电磁环境，体现具有活力对抗能力的交战实体，构设与未来作战相一致的战场态势，使对信息化军事人才在投身基地化训练中有实战感受。二是合理设置，发挥基地优势。组建高素质的模拟敌方部队，使信息化军事人才在激烈的对抗中磨练战术思想和

指挥能力；要组织好指挥训练、网上训练及实兵对抗等活动，发挥基地训练资源集约配置和先进训练方法的综合优势；运用科学合理的导调方式、评估系统，切实提高信息化军事人才的实战能力。三是紧贴实战，深化综合演练。要针对一体化联合作战中重、难点的问题，组织部队进行综合演练，练组织、练技能、练协同，提高人才的组织指挥能力，加深信息化军事人才对作战流程的理解，并就信息化武器装备作战前瞻性问题的研究，深化细化具体行动和战法，以培养信息化军事人才的创新意识和创新能力。

#### 参考文献

- [1] 转型中的军事教育与训练. 柴宇球主编. 北京：解放军出版社，2004 年
- [2] 世界新军事变革概论. 林建超主编. 北京：解放军出版社，2004 年
- [3] 2005—2006 年解放军报若干期

#### 作者联系方式

通信地址：合肥市电子工程学院研究生管理大队

邮政编码：230037

联系电话：0551-5767672

# 浅谈一体化训练中的信息化人才培养

华雪 夏逸平 梁龙喜

**摘 要：**一体化联合作战的本质是信息的集成与融合，作为作战的主体，信息化人才是打赢一体化联合作战的基础，一体化训练过程中，要正确认识信息化人才的地位和作用，综合集成院校、部队、科研单位等各种优势教育训练资源，发挥部队与院校两个渠道的作用，大力培养和造就信息化的人才群体。

**关键词：**一体化训练；信息化人才；人才培养

人才是一体化训练的主体，也是一体化训练的第一资源，更是一体化训练得以发展的重要基础。一体化训练的根本目的，就是提高我军遂行战争行动的能力，提高广大官兵以信息技术素质为核心的综合素质。

## 1 正确认识信息化人才的地位与作用

目前，部队在探索一体化训练中，普遍存在着忽视人的作用的倾向。有的同志认为，“我军半个世纪以来的军事训练实践都是解决人与武器的结合问题”，而当前的一体化训练是“由解决人与武器的结合向实现系统集成、体系融合的方向发展”，而不是解决人与武器的结合问题。这种认识是应该加以纠正的。尽管现代战争的形态正由机械化战争向信息化战争转变；尽管作战的基本形式将由协同式联合作战向一体化联合作战方向发展；尽管军事训练必然由协同性联合训练向一体化联合训练深化，但是，无论“系统集成、体系融合”到何种程度，都不可能导致人与武器的关系发生根本性变化，都不可能改变人在战争和军事斗争准备中的主体地位。系统的集成、体系的融合最终都要通过人来实现。因此，人才问题对一体化训练具有两方面的意义：一方面，探索一体化训练，需要有一支高素质的指挥员、参谋人员、专业技术人员、教练员和士官队伍；另一方面，必须以一体化训练为基本途径，锻造一支能够打赢未来信息化战争，加快我军机械化、信息化建设的、具有良好的全面素质、复合的知识结构和综合能力、较强的创新精神和创新能力的高素质信息化人才队伍。一体化训练如同任何形态的训练一样，也必须从最基础、最根本的

问题——“人”这一因素抓起，通过一体化训练，培养、发现、使用 and 造就能够实现“系统集成、体系融合”的信息化人才，促进一体化联合作战能力的生成和提高。培养和造就大批高素质信息化的军事人才，要综合集成院校、部队、科研单位等各种优势教育训练资源，发挥部队与院校两个渠道的作用，加快实施人才战略工程。

## 2 大力培养和造就信息化的人才群体

推进有中国特色军事变革的核心是信息化，未来战争的特点是信息化，一体化训练的技术基础也是信息化。在信息化时代，由于电子计算机的广泛运用，信息技术与数字化部队一起，彻底改变了作战与训练的方式，使军事人才群体越来越具有信息化的特征。如果没有一大批掌握和熟悉信息技术的高素质信息化人才群体，就难以创造、掌握和运用逐步信息化的工程装备，也就难以赢得信息化战争。信息化人才是有特定内涵的，一般来说，所谓高素质信息化人才，是适应信息化建设和打赢信息化战争要求的、具有良好信息素养的高素质人才。信息素养包括信息意识、信息知识和信息能力三个主要方面。信息意识是人们在信息活动中产生的认识、观念和需求的总和；信息知识是一切与信息有关的理论、认识和方法，包括传统的文化素养、军事专业知识和现代信息技术知识；信息能力是有效利用信息设备和信息资源，来获取信息、加工信息和有效利用信息的能力。目前，我军装备的有许多信息化程度高，技术含量高的新装备要掌握这些新装备的战术、技术性能，实现人与装备的最佳结合，需要具备较高的信息技术素养和广泛的知识

面。因此,装备越先进、越完善、信息化程度越高,越要求军事人才队伍熟练掌握信息化的技术手段,成为操作、使用、维修复杂高技术工程装备的“能工巧匠”。目前,我军部队中懂得信息化作战与训练的信息化人才比较匮乏。长期以来,由于培训机制不够完善,部队干部队伍的知识来源比较单一,知识面比较窄,对一些高新技术装备的战技术性能知之不多,不会操作使用;兵种之间、各专业之间换岗锻炼的机会较少,对本专业以外的作战指挥与训练程序不很清楚;跨兵种转换岗位锻炼也缺乏有效机制,能力素质的复合程度不够。人才队伍不适应新的训练方式的问题成了制约一体化训练的“瓶颈”。因此,要着眼一体化联合作战训练的需要,大力加强“五支队伍”建设,切实把提高官兵的信息技术素质作为一体化训练的核心,重点抓好指挥员、参谋人员、教练员、专业技术人员和士官的培训,培养和造就一批懂得信息技术、懂得一体化联合作战理论、掌握一体化训练组织实施方法、熟练运用信息系统的信息化人才,为一体化训练提供人才和智力支撑。

### 3 院校要发挥培养信息化人才的主渠道作用

院校是培养和造就人才的主渠道,要适应军队机械化、信息化建设要求,认真贯彻第十五次全军院校会议精神,以岗位任职为导向,加快由学历教育为主向任职教育为主转型。

#### 3.1 搞好人才培养方案的总体设计

按照逐级培训的要求,探索“订单式”特殊人才培养模式,尽快形成适应一体化联合作战训练需要的“训用一致、院校与部队相结合”的岗位任职教育新体制。

#### 3.2 深化教学内容改革

更新课程设置,调整教学内容,及时把信息技术的最新成果纳入教学内容体系,加大信息技术知识、一体化联合作战理论、一体化训练组织与实施的教学。要面向部队岗位任职需要,把科技素质、信息素质、创新素质和联合素质培养摆在突出位置,加强现职干部的工程装备操作技能训练和信息

技术技能训练,建立起与培养信息时代军事人才队伍相适应的现代化教学体系,加快培养一批懂得信息技术、懂得一体化联合作战理论、掌握一体化训练组织实施方法、熟练运用信息系统的指挥人才。

#### 3.3 加强学科专业建设

集中精力建好一批与一体化训练与我军现代化建设密切相关的学科专业,开发一批代表信息化条件下我军发展方向的新专业,逐步形成布局合理、具有特色和优势的学科专业体系。

#### 3.4 加强实践性教学

加强作战实验环境建设,既要重视现地教学和技术模拟,又要重视作战试验模拟,使教学环境尽量接近实战,努力提高学员对一体化训练环境的适应能力。

#### 3.5 加快教员队伍知识结构的更新

使教员队伍的知识结构尽快适应培养一体化联合作战训练急需人才的要求。要抓紧培训一批懂得一体化联合作战理论、掌握一体化训练组织实施方法、熟练运用信息系统的学术带教员,认真组织他们备课试讲,先为中级队学员开设讲座,为培养部队转型训练的人才准备好教学力量。

### 4 部队要发挥培养信息化人才的主阵地作用

部队是信息化人才成长的大课堂。要着眼一体化训练的需要,充分发挥部队培养和造就信息化人才主阵地的作用,把提高信息技术素质作为人才培养的重要内容,立足部队实践,加强岗位练兵,实现岗位成才。一是要从各级领导和机关抓起,采取送学、集训、专题研讨或者委托院校举办学习班等形式,突出联合作战和信息知识的学习,重点培训一批具有联合指挥素养的指挥员和参谋人员。二是要按照“依托上级,立足本级”的原则,采取理论学习和技能培训相结合的方式,重点抓好教练员、专业技术人员以及技术士官的培训,培训一批懂得信息化训练方法与手段、组织和实施一体化训练的人才,使之成为融入一体化训练的探索者和骨干力



量。三是强化信息化系统操作培训，充分利用办公自动化系统，音、视频教学系统等现代信息技术构建的网络练兵平台，积极开展网络训练，培养一批掌握指挥自动化系统、能通会连的信息化开发、管理、应用和操作的人才。四是立足岗位练兵，认真组织官兵学习信息化知识、掌握信息化装备，加强信息技术技能的训练，全面提高官兵以信息技术为核心的现代科技素质，使他们真正成为一体化训练

实践探索的主力军。五是部队要加强与院校的协作，广泛开展各种形式的共育人才活动，努力实现人才培养在院校教育和部队训练两个阶段相互联结，相互渗透，形成育人合力，真正建立起“人才共育，训用共管”的新体制，使一体化训练的过程成为培训人才、发现人才、使用人才、造就人才的过程。

#### 参考文献（略）

#### 作者联系方式

联系地址：江苏徐州解放军工程兵指挥学院四系筑城教研室

邮政编码：221004

联系电话：0516—83150664 13814437724

# 依靠“四个转变”优化院校育才模式

李恩忠 李彬 张程

**摘 要：**院校教育是培养人才的主渠道，院校育才要体现时代性，满足军事斗争需求，依靠实现育才观念、育才队伍、育才环境、育才周期的转变，优化院校的育才模式，提高院校育才质量。

**关键词：**院校教育；育才质量；转变

胡主席强调“要加强培养高素质新型军事人才，为军队信息化建设和作战提供强有力的人才和智力支持”。高素质信息化人才是决定新军事变革成败的战略资源，院校教育作为我军培养信息化人才的主要渠道，对于推进信息化人才培养具有基础性、全局性和导向性作用。在我军由机械化向信息化跨越式发展的关键时期，同时也是人才培养的重要战略机遇期，院校育才工作更应该走在前列，按照遂行军事斗争准备任务和履行历史使命的具体要求，通过实现院校育才观念、育才队伍、育才环境和育才周期的转变，推动人才建设的跨越式发展，提升人才培养质量。

## 1 做到“三个统一”，促进育才观念由分数、保守型向能力、开放型转变

育才观念是认识人才、培养人才、评价人才的出发点。军队信息化内容丰富、外延广泛，按照传统的以分数作为评价人才质量标准的育才观念，已难以培养复合型、多能型、专家型信息化人才。观念决定出路，要以发展的眼光、战略的高度来培养人才和检验人才。

### 1.1 全面培养与个别淘汰相统一

相比美国西点军校在校学员 20% 的淘汰率，我军院校生长干部学院淘汰率太低，一般情况下没有严重违纪不会被淘汰，导致学员学习积极性、主动性大大下降，能力、素质提高不大，达不到部队的用才标准。全面提高学员的综合能力固然重要，但若缺少良性竞争，必然会导致培养的学员良莠不齐。要以对军队信息化建设高度负责的态度，摒弃分数决定论，以科学的素质教育观、创新教育观、

超前教育观和开放教育观，多出懂技术、会管理、能指挥的复合型人才。同时，按照军队院校学员培养要求，坚持公平、公开、公正的原则，坚决淘汰不合格者。

### 1.2 培养共性与发展个性的统一

人才的成长过程和方式都是个性化和多样化的，应避免朝着整齐划一的方向“塑造”学员。在培养了学员高度的组织纪律性，一致的、循规蹈矩的军事技术技能的同时，也要尊重人的个体价值和能力差异，根据学员的特点和需要，拓展教学内容，以启发式、实践式、自主式、案例式、网络式教学方法强化学员的主动学习意识。以发展学员良好个性和特长为出发点，改革选修课和活动课，构建有利于学员个性发展的特色的选修课和活动课教学体系。加强教育引导和帮助，为学员的个性化成长创造更宽松的时间、更多的机遇，为个性发挥、施展才华、释放能量创造条件和搭建舞台。

### 1.3 理论学习与教育实践的统一

要树立与时代发展相适应的正确学习观，彻底改变“我讲你听”的灌输式教学方式，把学员看作教学过程中的主体，不仅使他们成为知识的接受者，更要成为知识的探究者和创造者。“实践是检验真理的唯一标准”，理论创新要在实践中得到检验和发展，要防止出现重理论轻实践、重概念轻应用、重说教轻研讨的现象。通过组织学员到部队实习、参观见学、模拟演练、学术研讨等形式，利用计算机网络、虚拟现实、模拟仿真等信息技术，将学员的新理论与新装备、新技术新战法结合，指挥管理和技术结合，学术研究和军事应用结合，从实践出真知，从实践出才干。

## 2 坚持“三个强化”，促进育才队伍由数量、规模型向质量、创新型转变

学员是院校教育的主体对象，教员是院校建设的主体力量，也是育才队伍的主力军，必须突出教员在办学育人中的主体地位，促使教员转变传统角色，自觉从知识的灌输着和对学员的支配者转变为教学活动的指导者、全面发展的促进者、学习创新的推动者，不断提升教学的品质、水平和境界，使军队院校的教学始终充满生机和富有活力。

### 2.1 强化教员的任职教育能力

第十五次全军院校会议提出了军队院校由以学历教育为主向以任职教育为主整体转型的发展目标，教员也要强化任职教育能力以满足院校转型的客观需要。建立教员下部队代职锻炼制度，尤其是装备技术与指挥管理类教员要有部队工作经历，了解未来信息化作战对人才素质的要求，培养人才才能真正做到因“材”施教。加大教员队伍的交叉培训力度，进一步开阔视野、丰富经历、积累经验、完善综合素质，增强任职教育能力。

### 2.2 强化教员的优胜劣汰意识

人的潜能发挥多少直接决定工作效率的高低，要依靠制度机制，强化教员的优胜劣汰意识，激发教员工作的热情和潜能。畅通晋升分流渠道。依靠专业技术职务任期考评制度，构建伯乐“相马”、教员“赛马”、学员“评马”的三马评价机制，公平竞争，坚持不惟学历、不惟资历，不惟身份，优胜劣汰，合理分流，防止教员队伍人才“泡沫化”。健全奖惩机制。奖励工作向教学科研一线倾斜，把工作实绩与切身利益挂钩，坚持物质奖励与精神奖励并举，善于发现、总结和宣传先进典型，特别是对完成重大任务、取得优异成绩者给予重奖，在教员中形成求真务实、争创先进的良好氛围。

### 2.3 强化教员的主动创新意识

主体是具有认识和实践能力的人，教员和学员都是教学活动的主体，教员是教的主体，学生是学的主体，同时也是教的对象和客体。在教育理论创新和院校改革发展过程中，教员扮演的是观念性领

导者的角色，他们既是知识的传递者又是创新和发展的引导者和促进者，他们改革创新的态度和行为，直接影响学员的创新思维。鼓励教员学习教育创新理论，改革教学内容和教学手段，积极推进科技自主创新。大力提倡勇于创新、敢为人先、敢冒风险的精神，为教员创新搭平台，营造鼓励教员创新，帮助教员创新的良好氛围。

## 3 实现“三个合力”，促进育才环境由独立、封闭式向联合、开放式转变

随着信息化时代的到来，各种知识和信息不断涌现、加速更新，院校育才也要最大限度的占有“信息的主导权”。教育资源是院校生存发展和人才培养的基本条件，目前，办学规模扩大、培训任务增多与教育资源短缺的矛盾，成为院校发展普遍面临的现实难题。院校自身资源的相对有限与学员要求掌握新知识、新信息、新技能的迫切需求之间的矛盾日益凸显，这就要求院校育才模式必须由独立、封闭式向联合、开放式转变。

### 3.1 院校——院校合力育才

现代知识的交叉重组、军事技术的飞速发展、未来战争综合力量的集成运用，使院校教学由小专业、窄口径、单纯追求某一学科知识的全面性和完备性向厚基础、大专业、宽口径、更加强调学科的综合性和整体性发展，美军“西点无专业”就是典型代表。这种趋势要求院校实行联合教学，统筹院校间的资源，改变以专业、学科和系来划分的相互割裂的纵向教学结构，创造超越单一学科背景的开放式教学体系，实现军事指挥、政治工作、后勤和装备保障的复合，指挥、管理和技术的复合，学术科研和军事应用的复合，以适应未来战争对军事人才复合素质的需求。

### 3.2 院校——部队合力育才

当前军队院校对人才的培养，在某种程度上看与部队需求脱节，满足不了部队管理教育、训练指挥要求。要培养复合型、多能型、专家型的信息化人才，院校应该主动协调对口部队，有计划地组织学员到部队调研、实习和代职。借助总部、军区机关的作战指挥中心，模拟实操演练，借助训练演习

等重要时机让学员参与,使其充分了解未来信息化作战对人才素质的要求,学到岗位任职所必需的知识和能力,特别是要了解新装备发展趋势、部队教育管理、训法及战法改革实际。部队也可选派经验丰富、素质高的优秀干部到院校介绍部队情况,甚至任教,充实院校育才队伍,对人才的知识结构与应用能力进行高层次、超前性培训,为其教学、训练提供依据与技术支持。

### 3.3 院校——地方合力育才

在军队信息化建设和未来信息化战争中,起支撑作用的信息技术具有军民结合的显著特点,可充分利用国民教育尤其是重点高校师资、专业、科研等优势,为军队培养出起点高、知识面广、技术过硬的高素质信息化人才。美军在地方大学设置的军官培训机构——后备军官训练团,已成为美军军官培养的主要来源,每年新任命军官有超过60%来自后备军官训练团(陆、海、空三军的比例分别为75%、40%、50%)。院校可直接从地方高等院校选拔吸纳信息化人才,对他们实施信息化指挥训练,使之成为技指合一的人才。进一步扩大国防生的培养规模和层次,委托有条件的地方高等院校、科研院所、博士后流动站为军队代培国防生,聘请地方专家学者到院校授课,以缓解军事教育资源的不足,走一条低成本、高效率的捷径。

## 4 立足“三个保证”,促进育才周期由短期、阶段式向终生、递进式转变。

人才培养是一项长期的复杂工程,做好军事斗争准备,必然要加快人才培养步伐,但不能一蹴而就。要以人为本,科学培养,使人才能够不断学习掌握先进的理论和技术,始终保持时代性,不贬值,不褪色。

参考文献(略)

作者联系方式

通信地址:西安通信学院军队管理教研室

邮政编码:710068

联系电话:029-84706039 13709229485

### 4.1 保证人才发展的信息化方向

新型军事人才的总要求是“两个适于”,即适于军队信息化建设,适于打高技术战争和准备打信息化战争。院校育才应以“保持领先性、注重全面性、突出创新性”为发展方向,构建高度信息化的校园环境,加强教育信息资源库的建设,抓好教学信息信息系统的开发和利用,注重多领域、多学科、多技术的综合知识的传授,努力培养和造就“复合型指挥人才、科学型管理人才、专家型技术人才、复合型保障人才和创新性理论人才”。

### 4.2 保证教学内容的系统化更新

随着信息作战的深入发展,传统的兵团阵地战、线式作战样式已被非接触、非线性作战样式所取代,新的战法和作战样式推陈出新,发展迅速,要求人才必须具备现代化、综合化、信息化素质。院校育才要掌握高新知识的更新规律,推进教学内容的创新,以提高学员综合素质和创新能力为主线,拓宽专业基础课口径,加大综合性教学内容,充实现代信息战、电子战、特种作战方面的知识,提高培养人才的层次和质量,保证培养的人才与时俱进,始终站在高科技知识的前沿。

### 4.3 保证人才成长的持久型能力

“十年树木,百年树人”,人才培养是一项长期工程,投入精力、财力、物力可能不能有立竿见影的效果,必须遵循人才成长规律,把育才投入作为战略性投入,一级一级抓持续,一层一层抓落实,使人才“可持续增长”。叶圣陶先生说过“教是为了不教”,信息时代知识以级数日益增长,一天不学习就有落伍的可能,一名军人不可能总在院校里学习,院校培养出的不能仅是某个时刻、某个阶段的人才。要使学员掌握学习的本领,有活到老,学到老的精神,无论在院校还是走向部队,都有持久的学习能力和动力。

# 信息化人才培养应注重强化“五个能力”

李科海 韩云山

**摘要：**建设信息化军队，打赢信息化战争，必须大力推进我军信息化人才培养的变革。本文根据信息化建设和信息化战争新要求，提出要重点突出“五种训练”，强化信息化人才的“五个能力”，以推进我军信息化人才队伍建设。

**关键词：**信息化人才；训练；能力

## 1 突出战斗精神训练，强化坚韧不拔的意志能力

信息化人才是信息化战争胜负的决定因素，官兵的战斗精神准备是军事斗争准备的重要组成部分。为赢得未来战争的胜利，在争夺信息制高点的同时，信息化人才的培训还应该根据官兵思想实际，抢占战斗精神的制高点，突出战斗精神训练，强化坚韧不拔的意志能力。一是加强战斗精神教育。强化“当兵为打仗、准备为打赢”的思想，不断增强忠实履行我军职能使命的紧迫感责任感，打牢“军队永远是个战斗队”的思想根基；强化“军魂”意识，坚持党对军队的绝对领导，把思想和行动统一到党中央、中央军委有关做好军事斗争准备的一系列决策指示上来，时刻想打赢、谋打赢、练打赢，始终保持高昂的革命斗志和顽强的战斗精神。二是加强人生观培养。用爱国主义激励官兵，用革命英雄主义教育官兵，通过真人真事不断培养广大官兵奉献、忠诚、职责、荣誉的人生观、价值观，使广大官兵在维护国家主权和领土完整的军事斗争中不怕吃苦，英勇杀敌。三是加强心理素质训练。通过复杂、高强度的军事训练，强化官兵特别能吃苦，特别能战斗的意志品质，培养敢打必胜的革命信念，一往无前地去争取胜利；开展适应高技术条件下的心理战对抗训练，努力掌握实施心理战攻防的手段和对策，不断增强信息辨别力和心理承受能力，筑起牢不可破的心理防线。

## 2 突出一体化训练，强化联合作战信息保障能力

推进中国特色军事变革，建设信息化军队，打

赢信息化战争，迫切要求军事训练这一最活跃的领域率先变革。信息化人才的培训也应按照一体化作战要求，大力开展一体化训练，不断增强联合作战的信息保障能力。一是加强一体化组网训练。瞄准联合作战需求，按照“三军一体、机固一体、通指一体”的要求进行综合组网训练。积极开展利用有线、无线电台、卫星、散射、微波等通信手段，实现通信和指控系统与情报侦察、电子对抗、火力打击等信息系统无缝连接的综合运用训练。加强陆基固定通信平台与陆基移动通信平台、海上通信平台、空中通信平台、太空通信平台等各通信平台的融合互通训练。二是加强一体化业务训练。利用信息网络进行信息获取、信息判断、信息传输、信息处理和信息利用的一体化训练；各类信息共享训练；数据信息、话音信息、图像信息的融合训练；各军兵种信息系统、电子对抗系统、网络战系统、主战武器信息系统的融合训练，努力实现信息流程最优化、信息处理实时化、信息利用一体化。三是加强一体化供修训练。信息化战争，通信系统是交战双方首选的攻击目标，战场通信器材消耗必定十分严重，只有建立供修一体化的新型保障机制，才能最大限度的满足信息化作战的要求。因此，必须围绕供修一体，科学确立训练机制，训练上做到有分、有合、有交叉。加强部门、军地和军兵种之间的横向联训，形成上下一体、内外一体、三军一体的保障格局，不断提高抢通、抢修、抢建等能力。

## 3 突出应急训练，强化突发事件信息保障能力

应急作战是当前我军面临的一种重要作战样

式。应急作战进程快、多种样式交融和指挥控制实时联动的特点,要求战役(战术)级指挥信息系统必须具有与之相适应的快速反应、机动中通和灵活应变能力,以满足作战行动的快速性、连续性和多变性对信息实时传输的需求。因此,必须针对应急作战的特点,抓好应急指挥信息系统训练。一是瞄准现实需求。根据可能发生的战争和将要担负的主要作战任务,严格按实战要求设置训练课题、营造逼真环境和组织实施考核。注重作战对手的针对性和作战环境的适应性,重视实兵演练和野外训练。二是突出快速高效。应急作战决策果断,行动坚决,要求指挥信息系统力量展开快、组网快、沟通快。因此,要合理制定各种保障方案,强化训练,健全战备制度,搞好战备教育、值班和检查,在作战样式、作战行动和战场情况发生变化时,指挥信息系统及相关网系能够灵活重组、快速转换,以快捷灵敏的反应能力确保作战指令及时、有效地传递。三是加强效能评估。通过效能评估来检验对突发事件信息系统保障的应变能力,是改进训练的一个重要手段。只有通过客观的效能评估,才能及时发现训练中存在的问题,才能根据问题制定改进方案,不断提高应急作战战役(战术)指挥信息系统保障能力。

## 4 突出对抗训练,强化信息安全防护能力

在高技术战争中,夺取信息优势的较量空前激烈,特别是随着军事信息网的发展,单一物理防护已不能满足现代战争的需要,必须围绕提高整体综合防护能力的目标,加强全维空间的整体防护训练,实现防护预警、防护实施、效果监控、后果消除等防护行动的一体化。一是加强抗干扰训练。在信息系统防电磁辐射、建立电磁屏蔽控制系统、实现发信设备电磁辐射自适应定向与功率调节、加强无用电磁信号多级屏蔽和外来强电磁能量隔绝等内容上进行训练。二是加强抗摧毁训练。利用地下防护工程、自然地形地貌和野战防护装备,组织三军

战场大范围隐蔽疏散战役(战术)指挥信息系统的实战演练,做到保障隐而不露,形散而力聚。三是加强网络防护训练。组织网络防御训练,在建立网关、防火墙、终端加密、信道加密等内容上进行研究性训练,建立严密可靠的信息防护网络系统。四是加强信息攻击训练。在做好信息安全防护训练的同时,还必须加强对敌信息攻击的训练。除了训练传统的电磁干扰、物理摧毁外,特别要突出探索网络攻击训练,以瘫痪敌网络为目标,研究各种攻击手段,争取在未来网络中心战中处于主动地位。

## 5 突出非军事训练,强化多元信息保障能力

作战需求牵引是军事训练的基本着眼点。进入21世纪,我军在围绕遏制战争、处置危机、解决冲突、促进和平等任务不断拓展职能,把打击恐怖主义、维持和平行动、人道主义救援、抢险救灾等非战争军事行动纳入职能范围,部队任务日益多元化。与此相适应,信息化人才的培训也要着眼遂行多种任务的需要,注重谋求多元化的作战保障能力。一是加强反恐保障训练。恐怖事件种类繁多、活动隐蔽,突发性强,信息保障准备时限短,对机动能力的要求高。因此,必须针对各种复杂情况,周密制定各类通信保障预案,反复进行训练。反恐作战又是一项群众性很强的斗争,要加强整体协调意识,利用军地资源优势,搞好军警民联防联训。二是加强维和保障训练。维护世界和平一直是我军的使命,1990年以来,我国累计先后向联合国14项维和行动派出4000多人次的维和军事人员。维和行动远离本土,必须以无线通信、卫星通信为主。因此,针对维和特点,开展以无线、卫星通信为重点的信息系统训练,探索维和保障训法。三是加强非军事行动保障训练。维护社会稳定、抢险救灾、反毒缉毒和人道主义救援等非战争军事行动任务,保障课题新、突发性强、军地合作难于协调,因此必须根据非战争军事行动的特殊环境、特殊情况和特殊规律,通过相应的模拟训练来掌握。

参考文献(略)

作者联系方式

通信地址:西安市王曲镇西安通信学院通信指挥教研室 邮政编码:710068 联系电话:029-84706611

# 加强后勤一体化训练，加快后勤信息化人才培养

李晓燕 孙云

**摘要：**为培养适应信息化战争需要的后勤信息化人才，必须大力推广和发展后勤一体化训练。本文分析了后勤一体化训练对于后勤信息化人才培养的必要性，指出了存在的问题，并提出了相应的对策。

**关键词：**信息化；后勤；一体化训练

## 1 引言

从 20 世纪 90 年代开始至今，以美国为主导的四场高技术局部战争，已经把我们对战争形态的认识从机械化战争提升到了信息化战争。传统的后勤保障方式已经不能适应信息化战争的客观要求。面对世界范围内信息化战争形态的转变及挑战，我军必须加速信息化建设的步伐，后勤信息化建设则是其中的重要内容。因此，大力培养适应信息化战争需要的后勤信息化人才是决胜信息化战争的关键一环。后勤信息化人才，是指在军队后勤信息化工作中具有一定的专业知识、技能和创新能力，并以创造性的工作对军队后勤建设做出贡献的人，包括后勤信息化指挥人员和参谋人员，在后勤信息化人才的培养中，后勤一体化训练具有不可替代的作用。

## 2 后勤一体化训练的必要性

后勤一体化训练不是新生事物，在后勤部队、各级部队后勤单位的后勤训练以及后勤院校的综合实践教学中，已经得到了广泛的应用。不论是实兵演练，还是基于计算机网络的分布式综合演练，都是基于训战一致，贴近实战的思路，对于各级后勤指挥和专业保障人才的培养，效果显著，其必要性毋庸置疑。从培养后勤信息化人才的角度，后勤一体化训练的必要性体现在以下三点。

一是通过后勤一体化训练，可以督促受训者构建完整的信息化人才的知识结构。后勤信息化人才的知识结构，大体包括基础知识、军事科学知识和专业知识。通过后勤一体化训练，直接或者间接的

强迫受训者，必须强化学习诸如物理、数学、地理等基础知识，不然就很难正确高效的使用各种信息化装备、软硬件系统；后勤一体化训练可以直接检验受训者的军事理论素养，不懂军事后勤理论，不熟悉后勤指挥、后勤保障原则、方式、方法、程序和习惯，就很难将自己投入到训练的角色中；另外，诸如计算机网络技术、安全防护等信息专业技术，必须通过后勤一体化训练，受训者才能够得到充分的体验和认知。

二是通过后勤一体化训练，可以培养后勤信息化人才的新思维。思维是在表象、概念、基础知识的基础上进行分析、综合、判断、推理等认识活动的过程。信息化战争要求后勤保障要迅速、准确，战机稍纵即逝，如果不更新传统机械化战争后勤保障的传统思维方式，不仅不能抓住战机打击敌人，还会被敌人打得一败涂地。必须抓紧培养出一批适应信息化战争后勤保障需求，具有高素质和后勤保障先进思维观念，掌握先进保障方法的后勤信息化指挥人员和参谋人员。如何通过后勤一体化训练来培养培养后勤信息化人才呢？首先，通过后勤一体化训练，有助于培养后勤人员后勤信息化保障的观念。目前我军后勤的指挥和保障理论相对外军比较滞后，定性分析多、模糊概念多、经验判断多、可操作性差等情况还将在一定时间内存在，然而通过参与后勤一体化训练，可以直接感知数字后勤和精确后勤等训练模式。目前的后勤一体化训练软硬件系统，或多或少都引入了数据库技术、计算机模拟仿真技术等，软硬件系统的设计上都参考了部分数字后勤和精确后勤的最新研究成果，有助于受训人员建立感性的后勤信息化保障观念。其次，通过参与后勤一体化训练，可以帮助受训者掌握和灵活运用诸如一体化聚合方式、立体化投送方式、精确

化释放方式等新型后勤保障方式。信息化战争的来临,必然导致后勤保障方式革命性的变化,必须让我军后勤信息化人才从机械化战争后勤保障方式的禁锢中解脱出来,掌握信息化战争后勤保障方式。只有把信息化战争后勤保障观念和保障方式融会贯通的人,才能驾驭未来信息化战争的后勤保障。

最后,在后勤信息化人才的培养过程中,强调打好基础的同时,应更加注重实际技能的锻炼,纸上谈兵是无法培养出信息类人才的。“以练引教、以练促教”是信息类人才专业技能培养的最佳模式,它已被信息技术发达的国家所采纳。

### 3 后勤一体化训练的现状和问题

针对目前我军存在的不同级别、不同形式和不同规模的后勤一体化训练,笔者有以下几点认识。

一是训练的目标明确,方式方法趋于一致。目前我军后勤一体化训练的目标锁定在用模拟、仿真、虚拟和网上训练等先进手段代替落后的训练手段,实现训练手段的跨越式发展,组织多课题、多情况的网上演练,形象地展现信息化战争作战模式、组织指挥方式和手段,对后勤指挥的影响和要求等情况,使其在复杂、逼真的战场环境中练谋略、练指挥、练协同、练保障,以适应保障信息化战争的需要。

二是训练的组织实施做到了分工明确,科学合理,逻辑严密,效果明显。分析我军存在的不同级别、不同形式和不同规模的后勤一体化训练的组织实施,不能发现,已经初步呈现出专业分工的趋势,相应地,也锻炼了一批专门的训练团队,有的专门从事训练科目的想定编写,有的专门从事训练软件系统的研发,有的专门从事训练场地的技术和后勤保障,有的专门从事训练考核和评估。专业化分工合作带来的是训练层次和质量的提升,训练组织实施的科学和高效。

根据笔者的浅见,目前后勤一体化训练还存在一些不足之处,主要有以下四点。

1) 重程序,轻谋略。后勤一体化训练很好地解决了后勤指挥和专业保障程序的训练,让受训者把后勤相关的知识串了起来。但是在实际的组织实施中由于训练强度很大,时间密集,需要处置的情况较多,留给受训者思考、决策的时间很短。受训者往往为了完成规定动作,疲于应付,对于指挥谋

略和决策水平的训练提高是有欠缺。

2) 重文电,轻数据。训练中的想定文书和受训者的作业处置文书,在组训单位之间来回流动,从而推动训练的进展。受训者关注的是内容的正确性、规范性和文电收发的准确性,但是对训练过程中的数据变动、数据真实性以及对指挥命令的限制等,却往往没有清晰完整的认识。以笔者多次参与后勤一体化训练的经验看来,文电和真实数据往往匹配不上,受训者对于数据的变化,比较模糊,不够重视,“纸上谈兵”的成分还存在。究其原因,主要有:各级组训机构中没有设置数据维护的席位,更没有赋予其跟踪和维护数据变化的职责;训练想定和软件系统在数据交互的接合部上存在粗细程度、采集标准和要求不统一的情况。

3) 重作业,轻模拟。现有的后勤一体化训练系统,存在一个普遍的现象,就是指挥训练作业功能比较完善,模拟评估功能比较欠缺。主要原因是后勤涉及到的模型层次复杂,后勤指挥与后勤保障模型联系紧密,加上后勤模型的研究工作处于起步阶段,有些模型很不完善,因此造成了在实际的后勤一体化训练中,指挥作业训练的成分很重,模拟评估往往很有限,有时候甚至被取消的情况。

4) 各自为战,重复开发,数据、平台、标准不统一。由于各个单位抓后勤一体化训练的力度和方式方法都不一样,加上总后系统并没有统一配发后勤一体化训练系统,就造成了目前各个单位重复开发、各自为政的局面。

### 4 后勤一体化训练建设的相应对策

参考外军和我军基层部队及院校后勤一体化训练情况,以及目前模拟训练技术发展的趋势,在信息化条件下,今后我军后勤一体化训练的发展应该重点关注以下几个方面。

一是统一技术平台,统一数据交换标准,建立相对比较完备的后勤指挥综合数据库系统。

二是全面深入地应用后勤模拟系统,使其涵盖战场态势和作战行动的模拟仿真,后勤保障任务生成、后勤保障行动和防卫作战行动以及后勤保障态势的模拟仿真。后勤模拟系统能使整个训练系统信息闭环,数据逻辑关系更加清晰和完整,确保参训人员指挥决策能有理(理论支持)有据(真实的数据能全面制约指挥意图的执行),从根本上杜绝在



训练中胡乱处置情况的发生，另外模拟系统独有的态势回放和推演功能，能全程监控并记录训练的进展，便于对训练作出全面有效的评估，从而提高训练的层次和质量。

三是持续完善综合性公共战场环境子系统、后勤作业子系统和战场动态监控系统，在此基础上，强化后勤指挥辅助决策的功能。充分发挥后勤指挥辅助决策的功能，不仅可以提高后勤决心方案

生成的速度和质量，还能对部分后勤决心方案进行论证评估。在训练中，后勤指挥辅助决策能帮助参训人员，统计分析大量战场动态数据，及时准确地掌握我方后勤力量部署、后勤机动、后勤防卫和后勤保障等方面的整体情况，便于及时调整力量和修正错误决策，能大大提高后勤指挥的效能，从而增强训练效果。

### 参考文献

- [1] 张召忠著.《怎样才能打赢信息化战争》[M].北京：世界知识出版社, 2004.
- [2] 董子峰著.《信息化战争形态论》[M].北京：解放军出版社, 2004.
- [3] 高凯，潘竞科主编.《信息化战争后勤》[M].北京：国防大学出版社, 2003.

### 作者联系方式

通信地址：北京市海淀区万寿路 28 号院 62 楼 40218 室

邮政编码：100858

联系电话：13651090261

# 联合作战条件下通信兵一体化训练问题的探索

刘齐兵 王新民

**摘 要：**本文主要从更新思想观念、完善训练体系，革新训练样式、优化训练内容，贴近实战要求、创新训练方法和加强技能培养、保留人才队伍四个方面探索了联合作战条件下通信兵一体化训练问题，为接近实战条件下的通信兵训练提供了参考依据。

**关键词：**联合作战；通信兵；一体化；训练

十届人大五次会议上军委主席胡锦涛同志指出：“军事训练是推进部队全面建设、实现科学发展的重要着力点。……重点围绕建立健全联合作战指挥体制、联合训练体制、联合保障体制，进一步深化军队体制编制调整改革。”我军通信兵是信息化领域的生力军，是信息作战的重要力量，肩负着我军指挥自动化（C<sup>4</sup>ISR）系统的主要作战任务。近年来，尽管通信兵得到了空前发展，但军事信息系统作战效能毕竟还没有得到战争的真正考验，在战场环境下是否能为我军作战指挥提供可靠的指挥控制平台，这些都仍然是难以料定的。因此，只有在联合作战体制下，通过对通信兵训练内容、方式和手段进行不断创新，在接近实战条件下训练通信部队，才能达到军队未来作战对我军通信兵实战能力的要求。

## 1 更新思想观念，完善训练体系

更新思想观念，完善训练体系就是要正确认识现代战争中通信兵地位、任务和作用，在此基础上建立通信兵完整的训练体系，使通信兵训练有章可循、有法可依。通信兵是军队作战体系中的一个特殊技术兵种，它由于不直接参加战斗，军队系统内部过去一直将其视为作战保障部队。20世纪90年代初，以美国为首的西方国家利用高科技手段发动了海湾战争，指挥控制系统在战争进程中发挥了巨大作用，引起了世界各国的广泛关注。现代通信兵的任务和职责已经从单一通信保障扩大到军队指挥自动化、情报信息处理等方面，任务性质的转变促使通信兵从军队保障序列转变为战斗序列。所以，我们必须将自己置身于战斗部队行列，进行接近战场环境的通信兵训练，才能在未来战争中充分发挥

通信兵的作用。更新思想观念是联合作战条件下搞好通信兵训练的基础，完善训练体系是搞好通信兵训练的保证。

首先，完善训练体系要有组织上的保证。目前军区以上机关通信部门都编有专门的训练管理机构，集团军以下部队通信处、科编有专门参谋人员负责通信训练工作，较好的保证了通信兵日常训练。但是，联合作战体制条件下我军延用的管理体制使军、兵种各级纵向训练管理比较顺畅，横向协调训练管理则非常困难。除技术体制原因之外，如果没有联合作战条件下通信兵平时的训练，战时诸军、兵种的战场频谱管理、指挥网络规划、信息系统互联等方面就会造成混乱。因此，协调军、兵种之间通信训练管理需要有体制上的创新，需要研究、建立诸军、兵种之间的联合训练管理机制。

其次，完善训练体系要有一系列的训练法规支撑。我军通信兵在编写通信、指挥控制、等系统的战斗条令、装备野战手册等教材方面还存在一定差距，虽然部分系统和装备有一些类似的训练教材，但很不完整，还没有上升法规、条令的高度。譬如，我军有些比较先进的通信、指挥自动化和电子对抗系统，平时部队基本是按照技术手册进行训练，既没有战斗条令，也没有野战手册等可供参考的法规性教材，造成参训人员对系统战术运用不明确，人员配备不清楚，系统开通与撤出时间不确定，战场环境要求不知道等问题。因此，我们必须加强通信、指控、电子对抗等信息系统训练法规和战斗条令的制定，使通信兵在联合作战体制下的训练有章可循、有法可依，达到“练为战”的目的。当然，完善训练规范涉及的内容十分丰富，需要有一个循序渐进、不断完善的过程，为此，我们要把这项工作坚持下去，为通信兵训练提供一套符

合战时要求的训练法规。

最后,完善训练体系要有具体的单位去落实。当前我军通信官兵基础训练基本上由初、中、高级院校和通信训练大队完成,多年来,为通信兵输送了大量指挥和技术人才,保证了各项任务的完成,提高了通信兵正规化训练水平。但是,实战训练还没有正规训练单位落实,如符合联合作战要求的通信训练中心等,虽然我们可以通过联合军演进行实战化训练,但毕竟这种训练方法不能使实战训练经常化和正规化,而且,长期下去资金投入大,难以满足实战训练要求。委托军事通信院校和综合基本训练基地建立联合作战通信训练中心是一种解决通信兵实战训练问题的较好途径,当然从长远发展看通信兵应该建立自己的综合训练基地,建立各种作战样式的训练模拟和仿真系统,模拟各种战场环境,对通信兵部队进行带实战背景的轮训。

## 2 革新训练样式,优化训练内容

革新训练样式,优化训练内容就是要紧紧围绕一体化联合作战,探索通信兵训练新方法,充实通信兵训练新内容,实现训练形式和内容的统一,适应新时期我军机械化、信息化作战要求。现在,诸军、兵种联合作战已经成为现代战争敌对势力之间战争的主要作战样式,通信兵训练样式必须围绕上述变化进行训练,才能跟上时代的发展。

革新训练样式首先是要加强逼近战场环境的通信传输、指挥控制、电子对抗的训练,特别是要加强陌生地域、复杂地形、强电磁干扰、无既设通信、快速机动等条件下野战对抗性训练;其次是要加强诸军、兵联合作战的信息系统协同训练,特别是要加强军种之间、兵种之间异构通信系统、指控系统的协同训练;第三是要加强各作战环节军事信息系统的互连、互通和电子对抗训练,特别是要加强指挥控制系统开设、野战通信系统建立、最低限度应急通信、战场频谱管理、压制敌方通信等训练;最后是由于高技术装备的“脆弱性”,决定了军事信息系统存在着可能出现故障的小概率事件,因此,要在实战背景下通过整个信息系统的有效度来检验训练效果,而不是只根据单台设备、单条电路的可靠性来检验训练效果。

优化训练内容应该根据新时期国家战略、军事思想、作战样式和信息技术发展,对训练内容进行逐一审查更新,重新组合通信兵各专业训练内容,

逐步达到优化训练内容的目的。优化训练内容要从训练内容的适用性、合理性和完整性入手。适用性就是要一切要从实战要求出发选择训练内容,使训练内容符合我军新时期信息化作战的要求,训练内容应包括进攻和防御作战两种类型的通信兵组织运用,根据不同作战指挥形式(联合作战、合同作战、协同作战等)、不同作战样式(山地、荒漠草原地、水网稻田地、热带山岳丛林地、高寒地等)编排训练科目;合理性就是要根据不同层次通信指挥军官、技术军官和士兵确立训练内容,使训练内容具有较强的针对性。通信指挥军官训练内容重点应放在系统部署和作战运用上,技术军官训练内容重点应放在系统规划和配置管理上,士兵训练内容重点应放在专业技能和战术素养上;完整性就是要使训练内容的范围纵向贯串战略、战役和战术通信,横向覆盖通信兵的各专业,确保训练内容体系的完整性。

## 3 贴近实战要求,创新训练方法

贴近实战要求,创新训练方法就是要通过创新训练方法使训练更加贴近实战,真正贯彻军委首长的“将来仗怎么打,现在就要怎么练”指示精神。

贴近实战要求进行通信兵训练,应从一体化联合作战大背景入手,从指挥控制、情报处理、火力打击、多维防护、战勤保障等多角度出发,组织通信兵部队进行一体化训练。指挥控制方面的训练要以各级固定和机动指挥所为中心,以通信和计算机网络为重点,进行作战指挥、通信传输、网络互连、信息处理、辅助决策、信息显控等方面的指挥自动化保障训练,确保各级指挥控制信息准确、无误、及时的传递和共享;情报处理方面的训练要以天基、海基、陆基侦察、监视和遥感等实时信息获取、处理和分发为中心,进行视频、数据和语音等多媒体情报信息的通信保障训练,确保首长和指挥机关能了解敌我双方动态,实时掌握和感知战场态势;火力打击方面的训练要以各种战术指挥控制系统、作战武器平台和数据链系统为中心,优化海、陆、空、天、电各类打击力量,进行网络平台中心战的保障训练,提高作战体系整体综合效能。多维防护方面的训练要以防空(国家和地域)体系通信保障和电子对抗保障为中心,主要应以三个能力的提高为训练目标,即防空预警能力、瞬间动用有效防护力量能力和网络平台安全防护能力。战勤保障

方面的训练要以“精确后勤”、“即时补给”等现代保障理念为出发点,依托全军指挥自动化网和战术数据链系统,搞好后勤、装备保障的通信和指挥自动化训练,为形成我军现代物流配送、精确保障方式、建立军事供应链体系提供信息支撑。

贴近实战要求进行通信兵训练,必须进行训练方法的改进和创新,这样才能保证训练质量,提高训练时效,降低训练成本。主要应从五个方面改进和创新通信兵训练方法,一是发挥通信兵院校作用,采用学院式教育训练方法,提高通信兵基础训练质量。分期分批送通信兵军官和士兵进院校轮训,可以保证训练标准的一致性、训练质量的可靠性和训练水平的先进性;二是改变单一通信兵专业“松耦合式”单独训练方法,采用多通信兵专业“紧耦合式”一体化训练方法。从系统论角度出发组织通信、指挥、电子对抗多专业一体化训练,提高通信兵综合信息保障能力和协同能力。三是建立全军性通信兵训练中心,通信训练中心集中各军、兵种现役通信与指控装备,采用轮训方式有计划的组织技术骨干进行实际操作训练,提高训练时效,保证训练效果;四是开发和建立符合不同作战样式要求的通信兵训练模拟和仿真系统。训练模拟系统可以对通信兵的组织计划、系统配置、电子对抗等内容进行类似实战的演练,训练仿真系统可以对通信兵专业技能进行类似实战的训练。采用训练模拟和仿真系统还可以减少人员和设备投入,降低训练成本。可以将这些系统配置到各战区综合训练基地,也可以配置到全军通信兵训练中心,甚至可以配置到通信部队,以便于部队组织轮训。五是组织带实兵检验性演习,提高通信兵军事素养,验收实际训练效果。带实兵检验性演习是通信兵适应战场环境,进行联合训练必不可少的环节。由于这类训练成本高,所以应以通信兵装备发生“代差”时适时组织,验收新系统在作战指挥系统中效能。另外,也可以通过军事演习来带动通信兵实战训练。

## 4 加强技能培养,保留人才队伍

加强技能培养,保留专业人才就是要使我军具有一支技术精湛、思想过硬、能打硬仗的通信兵队

伍。加强技能培养首先应加强各级通信指挥军官参谋作业和运用现代军事信息系统组织保障的能力培养。要克服重文笔、轻技能的弊端。要加强通信指挥军官系统组织运用、系统网络规划、系统配置管理等方面的能力,要对战略、战役和战术层次的通信指挥军官分层次组织轮训,满足作战指挥对不同级别通信指挥军官的要求;其次,应加强各类通信专业技术军官的技能培养。除院校基础理论培训之外,应重点加强实际装备运用和系统操作技能培养。高级技术军官重点应加强系统管理、系统规划、系统设计、系统重组、系统互连、教学授课等方面的技能培养;中级技术军官应重点加强系统管理、网络配置、系统维护、系统开设等方面的技能培养;初级技术军官重点应加强系统开设、系统操作、系统保养、系统维修等方面的技能培养。最后,应加强对通信专业士兵的操作维护技能培训。由于现代军事通信装备十分复杂,义务兵服役期内很难完全掌握,所以,通信兵士兵培养应重点放在志愿兵的培养。士兵培训应重点放在系统开设、装备操作、装备维护、体能训练等方面,另外,在有条件情况下可以对战士进行“一专多能”的培养,如计算机操作、汽车驾驶等方面的内容,这样可以减轻通信技术兵种的兵源压力。

通信兵事业要发展,人才是基础,专业人才是通信兵的宝贵财富。要通过实践、训练、比武等形式选拔一批能力强、技术精、思想好的通信指挥和技术军官在重要岗位上担当重任。另外,由于通信兵专业的特殊性,士兵队伍流动性过大将不利于通信兵事业发展,所以,要特别加强通信专业志愿兵的骨干人才保留和培养,搞好通信专业士兵人才的储备。在通信兵专业志愿兵的保留上应把重点放在通信专业士兵上,而不是通用专业(如司机、服务人员等)士兵上。

联合作战条件下通信兵一体化训练问题是一个非常复杂的系统工程,不可能一蹴而就,只有坚持科学发展观,不断进行思想、理论、方法和技术多方面的创新,才能使通信兵训练适应联合作战的要求。

参考文献(略)

作者联系方式

通信地址:山东省济南市辛西路11-1号72671部队 邮政编码:250022 联系电话:0531-51662611

# 多数据链操作规程研究

罗强一 刘冰 景柏树

**摘 要：**随着数据链系统的不断发展，多种数据链协同作战已成为常见的作战样式，对充分体现了其发挥作战体系整体效能的优势至关重要。本文阐述多数据链操作规程的基本概念和构成要素，对如何解决多数据链的互操作问题进行探讨。

**关键词：**数据链；操作规程；接口

## 1 引言

数据链是一种特殊的通信系统，它通过与情报系统、指控系统和武器系统紧密交链，实时传输处理各种战场信息，极大地延伸了平台的态势感知能力，提高了部队的快速反应和机动作战能力，使作战部队间相互支援，从而高效地运用军事力量<sup>[1]</sup>。数据链是一种按规定的消息格式和通信协议，用于实时传输各种战场信息的数据通信系统。它通常包含格式化信息、通信协议和传输信道三大要素，主要用于传输处理战场态势信息、指挥控制信息和武器协同信息。

数据链操作规程规定了数据链系统的组织运用过程、网络设计与规划规程、网络建立与维护规程和数据交换规程等内容。多数据链操作规程则主要侧重于规定联合运用多个数据链系统时的接口设置和管理相关内容。

美军拥有大量先进的数据链装备，在近年来的几次局部战争中还发挥了重要作用。当然，数据链的高效使用离不开操作人员对其操作规程的熟练使用。美军的“联合多战术数据链操作规程”为美军联合使用 Link 11/11B 和 Link 16，发挥其巨大的作用提供了重要的指导。通过联合使用多个战术数据链系统，可以在多种指挥与控制系统、情报系统以及武器系统之间实时交换战术数据，也可以使多个作战部队间相互支援、协同行动，从而提高作战效能。“多数据链操作规程”也将对我军高效地使用多数据链系统具有重要的指导意义；也必将有利于实现不同数据链系统之间的互联、互通和战场态势信息的实时共享，充分发挥武器的作战效能，提高协同作战的能力。

## 2 多数据链操作规程的构成要素

多数据链操作规程对操作员使用数据链交换信息，提高数据链的作战效能具有重大的指导意义。其内容主要包括以下几个方面：

- a) 多数据链接口说明；
- b) 多数据链接口职责；
- c) 多数据链接口规划；
- d) 多数据链接口建立；
- e) 多数据链接口维护；
- f) 多数据链接口信息交换格式；
- g) 多数据链接口训练规程。

### 2.1 多数据链接口说明

对各有关数据链系统接口分别进行了技术说明，建立了支持数据链运行的各话音协调网的需求，并且定义了各军兵种战术数据系统通用的数据链能力。

接口具有连续交换空间、空中、陆上、水面和水下航迹信息的能力。另外，还可以交换友方单元信息、武器与交战状态信息以及其他战术数据，为联合指挥员及其所辖部队提供处于系统监视下的整个作战区域的战术态势信息，还为指挥员提供向下属发送数字化命令、向其他指挥员发送数字化请求的能力。

#### 2.1.1 接口要素

多数据链接口由接口单元、数据链路以及话音协调网三个要素构成。

接口单元是指通过数据链直接连接到一个或多个其他接口单元的战术数据系统。它可以向其所连

接的其他接口单元发送数据，也可以接收来自其他接口单元的数据。根据其所实现的通信功能，接口单元可以分为直接参与单元、转接单元和并存单元（可同时在多个战术数据链上发送数据，但不能在这些链路之间转接数据）。

数据链路包括基本接口和扩展接口。前者能够利用链间的数据转接在参与接口的所有接口单元进行完整、详细的战术信息和命令交换。后者主要用于交换有限的战术信息与指令。

话音协调和控制网是不可或缺的，并被视为整个接口的一部分，主要包括网管话音协调网和航迹话音协调网。

2.1.2 接口单元和接口配置

数据链接口配置中需要注意的问题有：

- a) 确定每个战术数据系统的地理位置。
- b) 如果使用了多条数据链路，必须选择一个单元用于在使用不同数据链路的作战单元之间转发数据。
- c) 为接口配置提供备份能力，以确保当单个单元毁伤时不致造成信息流终止。

2.2 多数据链接口职责

多数据链接口职责描述使用数据链通信时的启动、执行以及终止操作职责。当多个战术数据系统通过数字接口链接在一起时，各个系统在功能上也联系在了一起。一个系统中的某些行为会对其他系统的 IU 的某些部分或整体产生一定程度的影响。这种数字互连方式实现了前所未有的互操作性。每一个战术数据系统再也不能仅简单看作是与其他单元交换信息的自治单元。必须对接口操作进行集中指导和协调以防止所交换的信息出现破坏性的冲突。多链操作通常在联合部队及其以下级别中发生。联合指挥员负责联合接口。联合指挥员一般通过作战参谋和通信参谋向网络协调管理组授权进行多链接口管理。网络协调管理组通过与各军兵种协调，负责建立接口和联合网络的初始功能，并负责之后的变更需求。网络协调管理组可以设区域网络协调管理组，以负责所分配的区域内的接口管理。

美军多战术数据链接口主要操作人员及其职责参见表 1。

表 1 美军多战术数据链操作人员及其职责

序号	人员	主要职责
1	联合特遣部队司令官	● 联合作战，包括战术数字信息链接口的全部权限及责任
2	密码主管	● 为联合特遣部队司令官协调战术数字信息链密码需求 ● 与 Link16 管理员一起管理 Link16 密钥变量 ● 与 Link11/11B 管理员一起管理日常加密模式和密钥变量
3	区域防空指挥官	● 分发作战任务链 ● 监控接口运行
4	接口控制官	● 规划接口协调所有接口参与者、军种与国家指导接口修改 ● 为区域防空指挥官建立作战任务链
5	Link16 管理员	● 协助准备作战任务链中 Link16 部分 ● 监控 Link16 的初始化、中继与运行确保遵循地方限制评估 Link16 的性能
6	Link11/11B 管理员	● 协助准备作战任务链中 Link11/Link11B 部分 ● 指定网控站、格网同步基准、数据链基准点、频率等 ● 确保 Link11/Link11B 的连通性 ● 指挥改变和校正行动
7	航迹数据协调员	● 协调实时的接口战术图 ● 协调点、线、面、过滤器、电子战数据转接模式 ● 监控解决航迹信息冲突 ● 发送变更数据指令 ● 指定跨链格网同步单元，并指导对格网同步单元进行的变更
8	专用信息系统管理员	● 充当话音产品网的网控站 ● 协调接口的信号情报信息 ● 协调接口情报报告

续表

序号	人员	主 要 职 责
9	军种代表	<div><div>● 实现联合接口要求</div><div>● 规定军种功能，并协调其需求</div><div>● 协助准备作战任务链</div><div>● 在各种的军种内准备并分发动令与计划</div></div>

2.3 多数据链接口规划

提供用于规划任意数据链接口所必须的公共规程，它应该适用于指导各参与数据链系统的接口规划。

规划过程主要包括评估所需的信息流和由此导致的连通性需求，确定可用来支持各种任务的数据链平台，制定满足作战指挥官需求的综合多链网络体系结构/接口方案，以及向作战单元提供实现多

链网络所必需的信息。

多链接口规划中最关键的要素是确定配置，以使用各种数据链将指挥与控制系统和武器系统有效互连，从而满足作战信息交换需求。还必须确定相关联的话音协调网的配置。选择完数据链接口配置之后，剩下的对于其他预先安排的数据项的规划就可以按逻辑进行。多链规划者用以支持联合作战的多链接口设计的典型步骤如表 2 所示。

表 2 多链接口设计典型步骤

编制需求文档	1、协调和获取设计接口配置所需的信息
	2、清楚定义接口网络的主要目标
确定可选配置	1、确定满足作战信息交换需求的可选数据链通信路径。主要限制为： <div><div>a) 指挥与控制系统和武器系统能力。</div><div>b) 数据链作战平台的地理位置。</div><div>c) 可用的通信设备和连通性。</div></div>
	2、提出作战设计考虑的事项。接口设计应该： <div><div>a) 战术合理、支持已有指挥与控制结构。</div><div>b) 使用与威胁一致的抗干扰能力。</div><div>c) 使关键节点数最少。</div><div>d) 使转发的消息流量最少。</div><div>e) 具有可选或备份连通计划。</div></div>
	3、 职责、任务和优先级与平台和数据链的能力相匹配
比较各可选配置并选择	1、在比较中考虑以下方面： <div><div>a) 实现目标和满足信息交换需求的程度。</div><div>b) 数据转发单元对消息流量的限制。</div><div>c) 可靠性。</div><div>d) 应急的灵活性。</div></div>
	2、对所需的折中进行评估
	3、选择最佳接口设计和配置
	4、对于降级运行提供应急方案
确定话音网配置	5、网管话音协调网
	6、航迹话音协调网

接口规划预先安排的数据项有：指定多数据链系统之间转发数据的单元，指定网络成员，指派网络责任，设置过滤器，分配编识号，并确定网络启动参数，生成网络配置参数并分发。

配置多链接口时还需要考虑的问题有数据链之间的数据转发，装备多链的各数据链平台同时进行的并行操作，以及链间基准单元的指定。

## 2.4 多数据链接口建立

提供建立多数据链的接口的操作规程。操作规程总的说通常适用于任何接口,而与具体使用的链路无关。当进行多链操作规划时,多数据链系统最初应该分别被单独建立。在开始数据转发之前,每个链应该被成功地建立。试图将降级的各链路进行接口很可能会中断操作。

## 2.5 多数据链接口维护

多数据链接口的维护包括转发单元移交、链路质量监测、数据注册和链路管理编码。转发单元移交是指当需要进行转发单元移交时,在转发单元和备份转发单元之间进行话音协调,备份转发单元在新的链路中成功建立其发送功能以及准备承担数据转发设备职责。在多链接口中,多数据链系统的主管人员分别负责监测各数据链单元的状态,并相应地指导状态和链路配置的变更。数据注册指本地和远端航迹位置数据之间相对对准的一种状况。当对于同一个接口航迹,所有接口单元本地导出的航迹位置数据都与该相同接口航迹的远端位置数据的测地位置相同时,可生成最佳的接口数据注册。链路管理编码是用于在隐蔽或公开的话音网上进行链路管理话音协调的简短语句或文字。

## 2.6 多数据链接口信息交换格式

多数据链接口信息交换格式适用于应用多数据链系统的操作。在联合作战中,根据功能分类,多链格式化消息包括系统信息交换和网络管理、平台

定位与识别、目标监视等信息,通常是各数据链消息格式的交集,需要依据相应的消息转换标准支撑各数据链消息格式之间的转换。

## 2.7 多数据链接口训练规程

训练与培训对于高效的指挥来说是必需的。需要按照训练与培训的情况进行作战。指挥官的技能在很大程度上依赖于其军事训练与培训的质量。多数据链接口的训练包括演习航迹和仿真航迹。其将使得在没有实际敌对方部队的情况下能够全面实现真实的作战训练想定。

# 3 小结

数据链在现代战争中有着举足轻重的作用,它是提升我军以数字化为基础的全军指挥自动化系统作战能力的关键之一,是赢得未来战争的重要保证。确保多数据链之间可以互操作,是提高数据链整体作战能力的关键环节。在解决多数据链互操作问题上,一是要加强数据链作战应用研究,把握多数据链联合应用的典型作战样式,理顺指挥关系与机制,在指挥层面上确保互操;二是要充分借鉴外军数据链建设经验,结合我军数据链建设实践,加快我军多数据链操作规程的研究与实现工作,加强数据链标准建设与互操作认证测试工作,在技术层面上确保互操作;三是要加强多数据链联合应用的演习、训练工作,提高应用水平,在使用层面上确保互操。

## 参考文献

- [1] 联合通信系统,总参第六十一研究所译,2006.03
- [2] The Joint Multi-TDL Operating Procedures,中国电子科技集团电子科学研究院译,2004.12
- [3] 16号数据链路使用手册,海军司令部通信部,内部资料
- [4] 兰汉平,丁锋,战术数据链技术现状及发展研究,舰船电子工程,2004年第5期

## 作者联系方式

通信地址:北京市丰台区大成路13号

邮政编码:100039

联系电话:010-66820008



# 信息化条件下的一体化训练

彭超

**摘要：**仗怎么打，兵怎么练。战争需求是军事训练改革的内在动力，规定着军事训练的发展方向。信息化战争形态的一体化特征要求军队必须通过一体化训练来提升一体化联合作战能力，确保军队掌握打赢信息化战争的主动权。

**关键词：**一体化；信息化作战理论；作战要素协调；信息网

## 1 一体化训练是检验我军信息化作战理论的客观标准

信息化作战理论的功能在于探索信息化条件下作战行动的特点规律，设计与构想“打得赢”的制胜之道。一体化训练所担负的一个重要使命，就是要检验我军信息作战理论设计与构想能否科学有效地指导我军信息化作战。

一体化训练将检验我军信息化作战理论是否适应信息化战争要求。先进的作战理论总是从战争实际出发，客观反映战争特点规律，科学指导战争实践。随着信息作战理论研究的深入，我军无论是在基础理论研究方面，还是在应用理论研究方面，特别是在如信息战、网络中心战、数字化战场、太空战等新领域的研究方面，都涌现出一大批在国内外有重大影响的理论成果。但是，这些成果是否能够准确反映一体化联合作战的发展规律，是真正具有指导作用，理论成果本身并不能回答这个问题，而只有实践才能回答这个问题。当我军尚不具备在实战中检验现有作战理论的条件，一体训练就成为检验的最现实和最根本的实践依据。

一体化训练是检验我军信息化作战理论正确性的重要标准。作战理论成熟的标志是理论体系的成熟。当前，我军军事理论界已经初步形成了信息作战理论的基本体系。但问题是这一体系尚处在理论研究层面，它的认识过程是否科学、体系结构是否严谨、原理原则是否具有真理性，还没有得到实践的全面检验。正是在这一形势下，一体化训练为检验我军信息作战理论体系的真理性提供了一个宝贵的契机。只有经一体化训练的检验，我军信息化作战的理论体系才能不断修改、完善和发展，最终形成权威、科学，具有我军特色的信息作战理论学

说，规范和指导全军的作战行动。

一体化训练将检验我军信息作战理论对外军的借鉴效果。由于我军缺少信息化局部战争的作战实践，我们的信息化作战理论研究实际上是在对美军和其他国家军队信息化作战理论研究和战争实践的基础上的。吸引外军的先进经验和研究成果，成为我军信息作战理论研究的重要方面。在这些理论成果中，哪些可以直接拿来为我所用，哪些可以供我军学习借鉴，哪些可以通过消化吸收变为我军自己的东西，都需要通过一体化训练来去粗取精、去伪存真、取长补短、为我所用。

同时还应看到，先进的理论只有为群众所掌握，才能焕发出新的生机和活力。从这个意义上讲，一体化训练将成为我军作战理论由研究性向群众性转变的桥梁，有了这个桥梁，中国特色的信息作战理论将在广大官兵的训练实践中不断完善和发展，并更加有效和迅速地向现实战斗力转化。

## 2 一体化训练是实验我军作战体制和编成的重要途径

一体化训练实质是通过信息技术的联能和融合，把分散配置的力量联成一体，高度集成的联合训练。它需要打破机械化时代作战编成的传统模式，以一体化联合作战为目标，建立高效指挥体制，大胆设计部队新的作战编成，在此基础上进行一体化联合作战实验。一体化训练的过程，实质上就是通过对各作战单元和作战要素进行编组配置，最终形成一支具有强大战斗力的一体化信息作战力量的过程。

通过一体化训练，有助于我军信息条件下形成一体化联合作战指挥体制。构建一体化的指挥体

制，是形成一体化作战力量体系的核心，也是开展一体化训练必须着力解决的关键问题。我军一体化联合作战的指挥体制研究该怎么建设，这个体制的机构编多大、职能如何界定、需要多少人员、配置什么指挥手段；它是否有利于对各种作战力量实施统一指挥，是否有利于达成对战场态势的有效控制，是否有利于实现各种指挥信息的快速传递与反馈，是否有利于建立实现平战快速转换的指挥体制，等等，这些不是依靠主观想象能解决问题的，需要在一体训练的实践中对各种方案进行检验论证。

通过一体化训练，有助于试验整合新型的信息化作战编组。信息条件下的一体化联合作战需要新的作战编成。在一体化联合作战中，火力单元与信息单元如何结合，各单元如何有效配合，最终形成有利于战斗力发挥的作战编组。各种预想的编组模式，只有通过一体化训练，把作战体系内构成作战要素的各种力量按不同功能模块的需要，打破建制进行编组实验，反复比较论证，才能得出正确答案。

通过一体化训练，有助于试验建立新型的作战单元。随着信息化战争深入发展，各种新的作战单元不断出现，并在作战中发挥越来越重要的作用。这些新型作战单元应该怎样建、建多少、建在哪一级、多大的编制，等等，这此不仅仅是理论问题，更是重要的实践性问题。这时，一体化训练就必然地成为这些新型作战单元生成的实践载体。通过一系列试点的方法，组建一批新型作战单元的实验部队，在一体化训练的“作战实验室”中进行实用性实验，可以充分积累经验，然后由点到面，全面推开。

### 3 一体化训练是磨合我军作战要素协调功能的最佳手段

近期几场局部战争的实践表明，一体化联合作战只有实现诸军兵种作战力量实体互动、结构耦合、功能互补，才能形成“1+1>2”的系统效应，没有各作战要素主动配合、协调一致的行动，将难以充分发挥各作战力量的整体效能。从我军建设的客观现实来看，积极推行一体化训练，不仅是提高我军一体化联合作战能力的必然选择，也是实现各作战要素功能协调的最有效手段。

开展一体化训练，将有助于磨合人员与武器装备系统之间的协调功能。人与武器装备的密切协同是一体化联合作战能力的基础。从我军目前的情况看，对于陆续配备的新型武器装备不会操作、使用，陆续建设的新型网络系统不会运用、管理的现象十分突出，极大限制现有武器装备系统的功能发挥，严重制约军队战斗力的生成与提高。因此，加强人与武器装备的协同、把人和武器结合起来就显得极为重要和必要，必须在加强人与武器装备的磨合上下功夫。而开展一体化训练，必将推动广大干部战士去熟练操作、使用、维护、管理手中武器装备，以充分发挥武器装备的战技术性能；推动广大指挥员去综合运用各种信息系统实施作战指挥与控制，以形成整体作战效能；推动各级领导干部去整体谋划各种新装备、新系统功能的发挥，以形成军队战斗力。

开展一体化训练，将有助于磨合诸军兵种之间的协调功能。诸军兵种之间的密切协同是一体化联合作战的关键。从我军当前情况看，军兵种内部、上下级之间的信息流还比较通畅，军兵种之间的信息共享则相对困难；诸军兵种之间对于配属、加强、支援关系还比较适应，对于临时编组指挥的意识则相对较弱；各军兵种按预定计划实施独立作战还比较顺利，依据任务需求实施动态协同则相对生疏。显然，诸军兵种之间的协同配合问题是我军实施一体化联合作战面临的最严重问题。这就要求我们必须把加强诸军兵种之间的协调放在突出重点的位置。而开展一体化训练，必须要求解决军兵种之间信息互联互通问题，以实现信息资源共享；解决诸军兵种在时间、空间、火力等方面的协同，以提高作战行动的一体化程度；磨合战役级指挥机关和指挥员对参战军兵种实施有机统一的组织协调功能，以综合发挥一体化联合作战效能。

开展一体化训练，将有助于磨合作战系统之间的协调功能。系统对抗是一体化联合作战的基本特征。这就决定着各作战系统的密切协同是一体化联合作战的重要保证。从我军现实情况看，情报信息、指挥控制、联合火力打击、综合保障等系统尚在构建之中，因而各作战系统之间的协同与一体化联合作战所需差距更大。在这种情况下开展一体化训练，必将促使全军去努力搞清有关作战系统协调的一系列问题，如各作战系统到底怎么协同、现有协同存在问题的原因在哪里、对这些问题应该如何

去解决等,对这一系列问题的解决,就必然有助于实现各作战系统之间的协同。

## 4 一体化训练是推进我军信息网络系统建设的强大动力

一体化训练是以一体化信息网络系统为依托,将一体化作战要素、诸军兵种作战单元融合成一体化联合作战体系,形成一体化联合作战能力的训练。显然,信息网络系统对一体化训练起着关键的支撑作用。随着我军一体化训练的推行,我军现有信息系统存在的“短板”效应、“瓶颈”问题和深层次矛盾将逐步显现。矛盾形成压力,需求产生动力,着力解决我军信息网络系统存在的矛盾和问题,必将对我军信息网络系统的建设起到强大的推动作用。

开展一体化训练,将为我军建立一体化信息网络系统提供强大动力。目前,尽管我军信息网络系统存在的问题已为人们所认识,但只有经过一体化训练的实践,才能使人们更加强烈地感受到,没有一体化信息网络系统的支撑作用,武器装备难于发挥整体作战效能,诸军兵种的作战行动难于协同,一体化作战体系难于形成,一体化联合作战能力也就无从谈起。一体化训练对于信息网络系统的强烈需求,就使得建立一体化信息网络系统成为全军上下的共同呼声。在这种共同呼声的强大舆论压力下,一切阻滞信息网络系统建设的“瓶颈”因素必然受到极大冲击,一些个人、一些单位、一些部门只顾局部利益而对信息网络系统建设形成的障碍也

将容易突破,从而必然推动我军一体化信息网络系统的建设。

开展一体化训练,将为加快我军一体化信息网络系统建设提供明确需求。建立我军一体化信息网络系统,必须首先明确其标准和要求,即必须适应一体化联合作战的要求。而信息网络系统是否真正符合作战需求,能否解决武器装备的信息控制问题、作战系统的综合集成问题、诸军兵种信息互联互通问题等,只有在一体化训练实践中才能得到充分地体现。一体化训练实践对于信息网络系统的功能需求与验证,必然有助于我们找准、搞清现有信息系统存在的问题,从而明确哪些通信技术需要改进,哪些通信装备需要发展,现有信息网络哪些功能需要延伸等,这就必然推动我军信息网络系统建设的加速发展。

开展一体化训练,将促使我军一体化信息网络系统建设迅速发展。在上述两方面分析的基础上可以看出,只有尽快建立我军一体化信息网络系统,才能为一体化训练提供根本前提和重要保证,才能提高我军一体化联合作战能力。在这种情况下,党、政府和军队各级领导对于我军一体化信息网络系统的建设必将更加重视,投入也将进一步增大,对信息网络系统建设的整体设计将更加科学,军地协同的联合攻关机制将形成,规模宏大的信息网络系统建设工程将展开,从而促使陆海空天一体化信息网络系统迅速建设,为各作战力量、作战单元、武器装备系统等要素有效融合为整体作战体系提供重要保障。

### 参考文献(略)

### 作者联系方式

通信地址:山西汾阳 61769 部队

邮政编码:032200

# 积极适应战争形态发展变化 努力推进战区一体化训练又好又快发展

戚小光 张继武 王万龙

**摘要：**本文对新形势下一体化训练的定义、内容体系、管理机制和方法途径进行了重点阐述，尤其是对搞好顶层设计，深化训练改革，建立完善与之相适应的一体化训练体系，提出了一定见解，为确保军事训练与时代发展和军事变革同步前进，实现打赢信息化战争根本目标，提供了一定理论依据。

**关键词：**推进战区；一体化训练；又好又快发展

科学技术的发展，战争形态的演变，使一体化联合作战成为现代战争的基本样式，客观要求军事训练必须朝着一体化方向发展。我们只有积极应对战争形态发展给军事训练提出的挑战，搞好顶层设计，深化训练改革，尽快建立并逐步完善与之相适应的一体化训练体系，才能确保军事训练与时代发展和军事变革同步前进，实现打赢未来信息化战争的根本目标。

## 1 更新观念，正确理解一体化训练的科学内涵

一体化训练，目前还没有全面准确的定义，一般认为，是为了提高部队一体化联合作战能力，综合运用各种信息技术、信息系统和信息资源，对作战系统、作战单元、作战要素、作战体系进行的综合集成训练。从一体化训练的大系统上看，一体化训练，属于作战单元内部集成训练，从通信的专业特性上看，本身需要构设完整的一体化训练内容体系，主要有三个基本特征。

**信息主导性。**通信兵一体化训练，离不开信息传输、计算机数据处理、网络联接等信息技术手段，构设贯通各作战层次、链接各作战要素的信息化平台，实现各子系统之间大量信息的安全、适时、交叉流动；需要通过信息系统的联通性和融合性作用，整合各装备系统、作战单元、作战平台等训练资源，优化训练编组、内容、方式、过程等训练实施环节，提高训练的整体效能。从训练的智力支撑上，离不开掌握信息化作战理论和专业技能的

新型人才群体；从训练的物力支撑上，离不开嵌入先进信息技术的武器装备和实现无缝链接的C<sup>4</sup>KISR系统。

**系统集成性。**通信兵一体化训练，一般是以单套通信装备子系统集成为基础，在横向上，包括电子侦察、干扰、防御等战斗单元集成，作战行动、指挥控制、作战保障等作战要素集成，电子战、网络战、火力战、心理战、特种战等作战体系集成；在纵向上，包括通信传输、电子对抗等分群内不同装备系统功能的集成，以及陆、海、空、天、二炮等不同军种通信力量形成完整的攻防体系的集成。无论是纵向上的联接，还是横向融合，都体现了系统集成性。

**整体融合性。**在训练目的上，为了生成和提高部队联合作战能力，更加强调将分散的各个作战子系统整合成一个新的系统，实现作战能力的整体跃升。在训练编组上，根据作战任务、武器装备及训练内容的变化，进行灵活的模块化编成，实现训练编成的横向和纵向的结构性调整，形成作战体系训练，提升训练层次。在训练方式上，由程序式过程训练向要素式、模块式整体训练转变，扩大训练范围，使通信部（分）队与其他作战力量更好地融合。

## 2 紧扣任务，科学构设一体化训练的内容体系

一体化训练从严格意义上讲，是从营（连）排级作战要素集成训练开始的，包括情报信息要素、

指挥控制要素、联合打击要素、综合保障要素等，这些既是支撑一体化联合作战的关键因素，也是构成作战单元和作战体系的基本要素。但又必须看到，作战要素集成训练与单兵、单件武器平台的基础训练有着密切联系。研究探索一体化训练内容，必须从基础训练抓起，以要素集成训练为核心，进行全面系统的改革。

**成系统一体化训练。**是指将通信部（分）队编成内装备系统，通过内部信息传输、处理、控制网络，进行各子系统装备的人机结合、逐步集成和互联融合训练，实现各类装备成系统形成整体作战能力。主要内容有，成系统配发的单套装备系统磨合训练和性能互补的同类系统装备整合训练。

**全建制一体化训练。**全建制一体化训练，是指在一定的战术背景下，以连级单位为基础作战单元，进行作战行动全过程的整体协同训练，提高全建制部（分）队的应急作战能力。主要内容有，作战单元内各子系统之间的战斗协同与融合训练；各作战单元与指挥控制单元之间情报信息传输处理与指挥协同训练；首长机关带各行动单元进行作战准备、集结机动、阵地展开、侦察预警、电子干扰、综合防护、野战生存、战场撤离等全过程作战行动训练。

**诸要素一体化训练。**诸要素一体化训练，是通信兵一体化训练的主体内容，是指围绕联合作战行动，通过强化各作战要素功能的集成，提升部（分）队整建制的整体作战能力。主要内容有，情报信息一体化训练，包括电子侦察分队的装备操作技能训练，指挥机关的情报信息系统技能操作训练，指挥机关带侦察分队进行的情报信息获取、传输、识别、处理技能训练，指挥机关与各作战单元进行情报信息安全防御训练，与友邻相关单位进行情报信息互通、共享训练；指挥控制一体化训练，包括指挥自动化系统的展开与联接，与上级指挥机关、友邻作战协同单位指挥自动化系统的分布交互式指挥协同训练，指挥自动化系统的安全防护训练，利用指挥自动化系统进行指挥作业全过程训练；综合保障一体化训练，包括通信部（分）队编成内作战单元与作战保障单元按照作战筹划行动全过程进行的协同训练，与上级及友邻保障单位之间的信息共享和指挥协同训练。

**整体系一体化训练。**是通信兵一体化训练的重点内容，是指围绕作战任务和具体战役战术训练课

题，打破现有建制，将电子对抗力量进行模块化编成，参加军种合成和诸军兵种联合作战一体化训练，形成和提升体系与体系对抗的整体作战能力。主要内容有，兵种作战体系一体化训练，包括通信部（分）队与预备役、院校、科研机构、地方相关单位的一体化联训，陆、海、空、天不同作战平台装备系统进行信息共享、指挥控制、预警探测、电子攻防等作战要素一体化融合训练；联合作战体系一体化训练，包括预警探测、指挥控制、综合保障等全要素作战行动一体化训练，组织战役筹划、信息作战、战役进攻、战役防御争过程联合作战行动和战法运用一体化训练。

### 3 统筹协调，建立健全一体化训练的管理机制

开展一体化训练，需要有一体化的训练机制作保证。当前，应按照立足现状、协作为主、强化职责、发挥优势的基本原则，尽快建立与一体化训练相适应的组织领导、训练管理和保障机制。

**一是要建立一体化训练的领导机制。**针对战区实际，当前可采取两种基本方式。首先，应建立战区性一体化训练机构。在现行体制编制下，由战区或战区内某一军种牵头，成立战区内诸军兵种参加的领导机构。第二是，应建立战术性一体化训练机构。由担负主要作战（训练）任务的部队或大型训练基地牵头，成立由参训诸军兵种部队参加的领导机构。这两个层次的领导机构，均应常设领导小组、办公室；战术性一体化训练机构可在一个战区内建立数个常设机构，也可根据年度训练任务临时组建。针对一体化训练参训对象多，层次、专业复杂，训练监控难度大等特点，着力提高训练管理模式网络化、手段自动化、内容规范化水平。管理模式网络化，就是要进一步加快战区内训练信息联网的步伐，按照横向到边、纵向到底的原则，实行综合组网、统一管理、互惠共享。管理手段自动化，就是要进一步加大训练管理软件开发与硬件建设力度，特别要综合运用计算机、网络通信、数据处理等技术，实现训练信息收集传递、加工处理、存贮应用的自动化。管理内容规范化，就是要进一步规范计划、登记、统计等训练信息资源和数据采集方式、格式、内容和标准，实现训练信息资源和数据的高度统一、标准制式。

**二是要健全一体化训练的保障机制。**针对一体化训练保障范围扩大、综合性增强、技术含量提高、地位作用上升等特点，努力实现三个转变：首先，是保障机构应由“分散型”向“联合型”转变。把目前分散编制在各级机关的训练保障机构整合起来，采取逐级设立或按区域、分方向设立的方法，组建诸军兵种共同参与、共同保障的联合训练保障机构。第二，是保障模式应由“封闭型”向“开放型”转变。打破军兵种之间、各层次之间训练保障孤立封闭、条块分割的状况，形成各类训练保障资源共享、综合组网、联供联保的新局面。第三，是保障内容由“单一型”向“综合型”转变。改变各类训练物资、经费以及技术保障多头管理和供应的状况，实现各军兵种和各类训练保障资源的统一管理、调度和供应，形成一体化的综合保障能力。

**三是要确立一体化训练的评估标准。**一体化训练评估标准，应重点围绕作战要素和作战单元、作战体系训练的集成水平来确立。其中，情报信息训练评估，应以网络互联互通的可靠度、获取和处理情报信息的准确率，以及传输和分发情报信息的时效率为基本标准；指挥控制训练评估，应以信息认知和判断的准确率、任务分配与决策的管理、发布与反馈指令信息的时效率为基本标准；联合打击、综合保障训练评估，应以获取共享信息和指令的准确率、接收和理解信息指令的时效率、实施打击与保障行动的有效性为基本标准；作战单元和作战体系训练评估，应以各作战要素之间的衔接与融合程度，作战单元、体系内部信息流动的顺畅程度，以及作战单元、作战体系内部联合行动的协调程度为基本标准。

**四是要改进一体化训练的评估方式。**当前，应着眼提高训练考核评定的整体性、联合性，从战区部队实际出发，采取三项基本措施。首先，是应实行联合考评。可分两个层次进行：第一层次为联合作战体系一体化训练考评。由战区或区域协作训练牵头单位负责，也可委托战区训练基地牵头，成立由战区内诸军兵种领率机关参加的联合考评机构，重点结合区域协作训练和基地化训练组织实施；第二层次为作战要素、作战单元集成训练考评。由军（师）级单位牵头，成立由各兵种部队领率机关参加的考评机构，重点结合首长机关训练和部队综合演练组织实施。第二，是力求训考分离。针对一体

化训练核心在指挥控制系统，审点在各级领率机关的实际，把训练考评机构与职责从领导机关自身分离出来，可在军区、集团军两级设立专门或临时性训练监督机构，履行对一体化训练监督和考评职能。第三，是注重整体评估。要着眼检验各类、各层次作战实体的一体化训练水平，注重综合衡量，实施全面评估。既要注重单个人员、单项课目的训练质量，更要注重作战平台、作战要素的训练水平；既要注重单兵种内部的集成训练质量，更要注重军种内部集成训练水平；既要注重战术训练质量，更要注重诸军兵种联合训练水平，谋求作战单元、作战体系集成训练质量的整体过硬。

## 4 大胆创新，积极探索一体化训练的方法途径

探索实践一体化训练，既要遵循军事训练的一般规律，按照先基础后应用、先兵种后合成、先军种后联合的思路来进行，又要针对一体化联合作战强调综合集成、体系对抗的特征，打破传统模式，改进组训方法。针对战区部队实际，当前开展一体化训练，应在充分利用大型训练基地、战区自动化网络等基础平台，广泛运用模拟化、网络化和对抗训练手段的基础上，按照以下几个步骤来进行。

**一是应进行基础训练。**主要以官兵分训的方式，按照两步进行。首先，是要通过理论学习，使官兵了解信息化战争常识及特点，掌握岗位专业理论，熟悉相关军兵种知识特别是信息化网络、设施、武器装备性能。第二，是要通过实际操作训练，使官兵熟练掌握手中武器装备，特别要精通信息化武器装备的操作使用，为开展单一作战要素、武器平台的内部集成训练奠定基础。

**二是应进行应用训练。**主要在兵种建制单位内部，分两步进行：首先，是信息网络应用训练应按照本级战役、战术信息网络的展开要求，组织受训对象按照岗位职责和任务区分，进行信息网络节点和信息分系统的互联、互通训练。其次，是信息传输与作战实体联接训练，按照战场信息流动要求，进行系统联接和信息获取、处理、发布等方面的实际操作训练，为开展作战单元内部集成训练奠定基础。

**三是应进行集成训练。**主要在军种内部，分三步进行。首先，是兵种作战要素集成训练。通常由

连（营）级单位或各级机关组织实施，重点围绕提高单一作战要素的侦察、预警、指挥、机动、打击、保障等作战能力，对单一作战要素、单一武器平台内部各个子系统实施集成训练，实现基本作战平台的集成。其次，是兵种作战单元内部集成训练。通常在军、师、旅、团建制内，采取分兵种（专业）集中组织的方法进行，重点围绕提高单一兵种（专业）的整体作战能力，对兵种内各作战要素、作战平台实施集成训练，实现单一兵种作战单元的集成。第三，是军种作战体系集成训练。通常以师、旅、团为单位整建制进行，重点围绕提高军种内各兵种专业部（分）队的一体化作战能力，对情报信息系统、指挥控制系统、战斗行动系统、火力打击系统、防空作战系统、战斗保障系统、后方

保障系统等，进行综合集成训练，实现军种作战体系的集成。

**四是应进行联合训练。**主要在军种之间，分两种方式进行。首先，是联合战斗群模块一体化训练。通常由战区专设训练机构或军、师、旅级单位，按照作战需求，以模块方式编组由多军兵种力量组成的作战集群，并以战斗群模块为单位的各军兵种作战系统实施集成训练。第二，是联合战术兵团或联合战役军团一体化训练。通常由战区或专设训练机构组织实施，以联合信息传输、联合信息对抗、联合信息控制、联合行动打击、联合实施保障为主线，组织诸军兵种首长机关或实兵一体化演练。

### 参考文献

- [1] 王文荣主编.《战略学》.北京：国防大学出版社，1999
- [2] 《正规化训练经验材料汇编》，总参谋部军训部，1993
- [3] 《通信兵训法改革与实践》.总参谋部通信部.北京：解放军出版社，1998

### 作者联系方式

通信地址：北京市石景山区八大处甲9号

邮政编码：100041

联系电话：010-66397806

# 信息化条件下装甲兵人才培养浅探

秦伟 苏鹏 何明

**摘 要：**信息化战争是一种新的战争形态，对装甲兵人才提出了许多新要求、新标准。在分析装甲兵人才培养存在的不足的基础上，提出了信息化条件下装甲兵人才必须具备的五项素质，最后给出了加强装甲兵人才培养的三种途径。

**关键词：**信息化；装甲兵；人才培养

## 1 引言

“人才为政事之本，也是建军治军之本。”所谓人才，从普遍意义上讲，是指那些在各种社会实践中，具有一定的专门知识、较高的智能，并能以自己的创造性劳动对人类进步做出较大贡献的人。在一般人才概念的共性范畴内，装甲兵人才就是指具有丰富的装甲兵方面的专业知识和极强的实践能力，能为进步的军事活动做出创造性贡献的优秀分子。信息时代和新军事革命的迅猛发展，对军事领域产生了全方位的、根本性的影响，给我国国防和军队的现代化建设带来了严峻的挑战，也对装甲兵人才培养提出了更高的标准和更新的要求。抓紧培养与装甲兵部队信息作战和建设相适应的人才队伍，已经成为当前我军装甲兵部队信息化建设的一个战略性课题。

## 2 装甲兵人才培养存在的不足

当前，装甲兵部队的人才素质滞后于部队信息化建设发展的要求。一是官兵科学文化基础比较薄弱。据统计，美国军官 100% 的是大学本科以上文化程度，其中硕士、博士研究生占 38.4%，参加海湾战争的美军军官中，三分之一的人员具有硕士以上学位；俄罗斯有 98% 以上的军官受过高等教育，日本军官全部达到大学以上文化程度，印度要求营以上军官必须获得硕士学位。而在我军装甲兵部队中，干部队伍虽然具有高度的政治觉悟，优良的思想作风和坚忍不拔的革命意志的突出优势，但是受过全日制大学本科教育和拥有硕士以上学历的军官占军官总数的比例较低，其中文科又占有较大比

例。这样大的科技差距是难以适应信息化建设要求的，所幸的是大家都已意识到人才培养是提高战斗力的关键之举。二是培养人才的起点不够高。不论是人才培养的目标定位、内容设置，还是人才的选拔使用上，都没有很好地转到军事斗争需要上来。我们长期生活在和平环境里，部队几十年没有打仗，大部分官兵没有实战的经历，更不要说现代战争的锻炼了。三是拔尖人才严重短缺。技术干部特别是既懂指挥又懂技术的复合型干部数量少，素质偏低，远远适应不了信息化条件下各种复杂的保障要求。在部队调查中发现，不少单位训练中遇到技术难题后，只好到地方院校、科研单位请专家；有些新装备配发到部队后，连说明书都看不懂，出现了新装备“趴窝”现象，因此信息化建设在部队基层遇到了很大的阻力。最主要的是信息化人才制度还不健全。优越的人才制度可以吸引人才、保留人才、凝聚人才，促进人才的快速增长，形成“环保型”可持续发展的人才建设模式。但是，目前的人才制度对信息化的重视还不够，形成“不拘一格将人才”的良好环境的速度还比较缓慢。

## 3 信息化战争对装甲兵人才培养素质的要求

信息化战争是人才智力的较量，是智慧的角逐。信息化战争的本质是人的信息素养的较量，对军人素质提出了新的要求。因此，着眼未来战争对军事人才素质的要求，装甲兵人才的培养必须着眼以下素质的提高，具体表现在：

一是具有优良的政治素质。在未来的信息战争中，指挥人员不仅要面对复杂的陆、海、空、天、电多维空间信息的处理，还要面对反分裂、反渗



透、反恐怖任务及强敌介入。一切军事斗争都可能与政治、经济、文化、外交、民族相交织，具有很强的政治色彩。因此，装甲兵人才必须具有正确的世界观、人生观、价值观及坚定的政治信念和大局观念，善于着眼国际大背景，以维护国家利益和捍卫国家安全为出发点，正确判明战争的性质和综合分析敌我政治、经济、军事等方面的矛盾。

二是具有较强的信息化指挥技能。随着装甲兵信息化武器装备技术含量的不断增大，信息化条件下的装甲兵人才必须具备专业化和知识化能力。要能通过多种方法、多种渠道采集信息，具有强烈的信息致胜信念；能熟悉敌我双方信息战武器装备的战术技术性能及现代高科技知识，具有较强的信息化处理水平；能熟练操作和控制与个人职责密切相关的现代指挥工具和武器装备，具有熟练的操作技能；能够熟练掌握处理信息的程序以及分发传递的各种方法，高效的处理和使用信息，具有较强的管控能力。

三是具有复合型知识结构。现在先进的坦克集信息处理、激光对抗、微光成像、数字火控等高新技术于一体，大量使用微光电子、激光、感测、计算机与智能技术及控制技术。这就要求装甲兵人才既要通晓信息技术、生物技术、新材料技术、航天技术、海洋开发技术等高科技知识，又能够广泛的运用军事谋略学、军事运筹学、数学、物理学、决策学、思维学、计算机作战模拟仿真技术等等，具备多学科、跨专业的系统综合知识。不仅要在本学科、本专业具有较深的造诣，还要对相关学科专业有较深的了解，具有较强的系统综合能力。

四是具有较强的科技创新能力。在未来的信息化战争中，由于参战单位和作战力量多元化，战场空间扩大，制约作战行动的因素增加，信息控制和信息探测装备增多，使得需要获取和处理的信息量剧增。作为装甲机械化部队信息化指挥人才，必须具有较强的专业技术知识和科技素质，能够在作战中大胆运用信息作战理论、自觉得依靠科技手段创新指挥方法。

五是良好的心理素质。现代条件下的信息作战强调速战速决，作战样式转换频繁，战争异常艰苦、激烈、紧张，使人的智力和体力消耗大增，指挥员在多数情况下要处理的不仅是物流，而且有大量的信息流。这就要求指挥员必须具备强健的体魄和良好的心理素质，善于在最艰苦、最紧迫和最恶

劣的条件下完成各项急、难、险重的指挥任务，能够做到处变不惊、临危不惧、关照全局、沉着应变和创造性的进行组织指挥工作。

## 4 锻造信息化装甲兵人才的主要途径

抓信息化建设，必须坚持牢固树立人才先行的观念，按照人才成长规律，超前培养，开放培养，把人才队伍建设作为战略工程来抓。应着眼信息化人才的总体需求，搞好宏观规划，使培养任务落到实处；应结合教育训练改革，优化人才知识能力结构，突出信息技术应用能力培养。既要发挥院校人才培养的主渠道作用，也要重视部队训练这一实践性环节，同时还要有针对性地引进地方信息专业人才，不断发展壮大装甲兵信息化建设人才群体。

### 4.1 树立“超前培养”的观念培养人才

超前培养，是指信息化战争的知识要先于战争实践积累，打赢信息化战争的能力要先于战争实践锻炼，驾驭信息化战争的人才要先于战争实践培养。一方面，军队信息化进程推动战术和技术不断演化和快速发展，知识更新周期大幅度缩短；另一方面，高技术局部战争节奏快、强度高、范围大、持续时间短，仅适应于机械化战争规律变化较慢的经验累积式的知识获取模式已无法适应信息化战争的需要。因此，在装甲兵人才培养过程中，必须树立超前培养的观念，以现实军事斗争需求为牵引，科学确定训练内容，实现信息化装甲兵人才与信息化武器装备及信息作战理论的有机结合。一是依据装备技术发展构建训练内容。随着我军武器装备不断更新，一些比较先进的新装备、指挥控制系统等陆续列装，必须把信息技术训练纳入部队基础训练之中，优化现行专业，拓展新型专业，注重新装备操作与使用，加大通信、计算机、指挥自动化与网络技术的训练力度。二是依据未来作战任务构建训练内容。未来作战是在复杂国际背景下的战略决战，只有瞄准强敌设置训练内容，按作战任务练兵，才能把兵练实、练活、练精。必须紧扣信息化战争要求，围绕“打得赢”，突出快速反应、信息对抗、协同作战和综合保障等内容，以适应信息化条件下作战的特点和要求。三是依据未来战场环境构建训练内容。根据未来作战样式可能的特殊作战

环境,进行信息战战法演练。

## 4.2 依托军事实践活动实施“多渠道、多岗位”锻造人才

目前,我军的合成化空前提高,繁杂的专业和丰富的岗位,是培养复合型军事人才的最好学校,装甲兵人才培养也应该融入到这所学校中来,拓宽培养渠道。一是实施换岗培养、交叉锻炼。要扩大数量规模,走出陆军,融入三军,提高跨军兵种部队交流轮换的层次;对重点培养对象搞“滚动式”锻炼,进行多单位、多岗位、多机会的摔打;以新装备部队为实践基地,学习新知识、掌握新技能、研练新战法,发挥新装备在人才培养方面的最大效益。二是在重大军事实践活动锤炼。一体化联合训练、演习等和平时期协同程度最高的军事实践活动,是培养复合型军事指挥人才的最佳舞台,其中,装甲兵也是一个重要的力量分支。世界各国都重视此法锻炼人才,把军事演习特别是合成部队的演习,看作是平时对军官最有价值的培训。美军每年由参谋长联席会议组织的大规模联合演习达50次之多。我们要善于借鉴外军的经验,拓宽依托一体化训练联合演习培养人才的途径,不仅让有发展潜力的干部充分展示自己的才华,而且还能把素质缺项的干部推到一线,在近似实战的环境中接受锻炼。三是送各类培训基地训练。各类训练基地介于部队实践锻炼和院校培养人才之间,是更加接近部队训练的一种培训模式,要善于发挥各类训练基地培养人才的重要作用,采取改训、代训、补训等形

式,提高装甲兵人才的综合素质。

## 4.3 借助国民教育优势从更大范围选拔培养人才

开放性是一个社会系统充满活力的基本条件。高素质装甲兵人才的培养和成长同样需要一个开放的教育环境。随着高新技术广泛应用于军事领域,军事专业越分越细,军队建设所需专业人才的种类越来越多。但由于种种条件的限制,军队院校又不可能全部包揽教育过程和所有教学内容,这就需要普通教育来弥补。世界上一些国家十分重视军队教育与国家教育的兼容与并蓄,将军官教育纳入到国家教育的体系中,在教育内容、方法、体制和人才等方面与国家高等教育挂钩。如美国的许多地方院校开办后备军官训练团,利用社会力量培养军事专门人才。军队院校教育必须向社会开放,必须加强与地方院校和有关科研机构交流与合作,疏通军校与地方院校之间的交流渠道,充分利用军地院校各自的优势,加强人才交流,互派专家教授讲课,广泛开展科研方面的合作,做到互惠互利,信息共享,充分利用全社会的科学技术成果来充实完善自己。积极创造条件,有计划地派一些教学科研人员及管理人员到国外留学、进修和访问,请外军专家来院讲学,广泛吸收世界新知识新技术,提高培训层次和教学质量。这种教育上的革命,将给装甲兵人才的培养带来了生机和活力,不失为一种有效的方法。

## 参考文献

- [1] 郭梅初. 高素质军事人才培养途径与方法[J]. 高等教育研究学报, 2000, (2): 24-28.
- [2] 夏中国. 紧跟中国特色军事变革走向加速培养复合型军事人才[J]. 军队政工理论研究, 2005, (6): 38-40.
- [3] 刘太平等. 论信息化战争对军事人才的素质要求及培养途径[J]. 思想教育研究, 2005, (12): 41-43.
- [4] 程谋学等. 信息化战争对人才队伍建设的要求及对策[J]. 军队政工理论研究, 2005, (2): 45-46.

## 作者联系方式

通信地址: 安徽蚌埠坦克学院研究生队

邮政编码: 233050

联系电话: 13695525691

# 信息化条件下军事人才培养评估

任在安 王斌

**摘 要：**信息化条件下的军事人才不但要有良好的政治素质，而且要具备与高技术条件下局部战争相适应的任职基础素质和良好的岗位业务素质，这就需要对指挥人才进行客观正确的评价，本文以炮兵院校学员为例，对信息化条件下的各个评价点运用模糊综合评判的方法进行评估，从而客观地反映学员的综合素质。

**关键词：**综合素质；模糊综合评判；评估

## 1 军事人才培养评估的依据

军事人才培养评估作为一种有目的、有计划、有组织的行为，在实践中要想有效地开展，必须有科学的依据。这些依据主要有以下几点。

### 1.1 军委、总部有关法规性文件

军委、总部遵照院校教育和人才培养的客观规律，对学员的培养教育做出了许多规定，颁布实施了一系列条例、制度等，如《中国人民解放军院校教育条例》、《学员学籍管理规定》、《关于做好在军队院校学员中评估优等生工作的意见》、《军队院校学员淘汰实施办法》等文件，这些文件是依法治校、依法治教的依据，也是院校进行人才评估的依据。院校制定培养目标，设置课程体系，衡量教学质量，必须以军委、总部颁发的关于院校教育、人才培养的有关文件为依据进行评估。

### 1.2 部队对军事人才的基本要求

军队院校的基本任务，就是为军队现代化建设和军事斗争准备培养高素质新型军事人才。针对世界格局与安全环境的变化，军委进一步明确了大力推进中国特色军事变革、建设信息化军队、打赢信息化战争的战略方针。军队院校也必须努力培养适应建设信息化军队、打赢信息化战争需要有过硬政治素质、合理知识结构、旺盛创新能力和坚强意志品质的高素质新型军事人才。军校军事人才评估必须依据这一总的基本要求，制订评估方案，确定评估标准，组织实施评估，提出评估结论，不能有任何偏离。

## 2 军事人才评估的作用

军校学员作为军校教育的对象，作为军校“生产”的“原料”和“产品”，作为军校教育教学过程的主体，对它的评估不仅涉及学员本身，而且涉及教员教学、学员管理以及院校人才培养的方方面面。军校学员评估对于促进院校各方面工作具有极大的促进作用，具体来说，有以下几个方面的作用：

### 2.1 调动学员的学习积极性

学员学习和训练的积极性是激发学员努力进取、克服困难、完成学习任务、实现教学目标的动力源泉。通过评估，学员可以从信息反馈的角度，正确认识自我的成绩与缺点，了解自身知识、能力、素质现状，明确前进的方向和目标，让学员看到自己与专业培养目标、与阶段性目标、与领导要求之间的差距，从而调动和激发学员求知上进的欲望，并将其转换为旺盛的学习热情。另外，评估还可能引起学员的焦虑。心理学的研究表明，适当的焦虑可以成为一种动机力量。这种动机可以激发学员学习的积极性。

### 2.2 为教员改进教学工作提供依据

教员在讲授新课程之前，要对学员的相关知识、技能、能力、学习态度以及学习方法进行了解。了解的基础就是各种对学员学业成就的评价。教员通过对学员学习前期准备情况的了解，在教学过程中，就可以采取针对性教学策略。在具体的教

学过程中，教员可以通过不断地对学员各方面进行评估，分析学员在知识、能力和素质方面的情况，发现教学计划、教学内容、教学方法、教学组织中的薄弱环节，从而有助于教员采取针对性的措施，更新教学设计，完善教学实施，优化教学内容，改进教学方法，以促进整个教学工作的改善。

3 军事人才评估的方法

3.1 模糊综合评判

所谓综合评判，就是对受到多种因素制约的事物或对象，做出一个总的评价。在我们日常的生活和工作中，无论是产品质量的评级，科技成果的鉴定，还是干部、学生的评优等，都属于评判的范畴。如果考虑的因素只有一个，评判就很简单，只

要给对象一个评价分数，按分数高低就可将评判的对象排出优劣的次序。但是一个事物往往具有多种属性，评价事物必须同时考虑各种因素，这就是综合评判的问题。由于在很多问题上，我们对事物的评价常常带有模糊性，因此，应用模糊数学的方法进行综合评判将会取得更好的效果。通过建立“多层次、多算子的模糊数学模型”用于多因素的综合评价，是对人们决策思维过程的数学描述。

3.2 多层次多算子二型模糊综合评判数学模型

本文以连排职初级指挥军官任职教育学员素质的3个方面，12个类型，22项详细项目以及相应的权重分配如下表：运用多层次多算子二型模糊数学模型进行综合评价，专家评审小组为8人。

连排级指挥军官任职教育（一年制）学员综合素质评估标准

一级指标	二级指标	主要评估点	评价等级					权重
			优秀	良好	中等	及格	差	
思想政治素质 20%	政治鉴别力 20%	对重大原则问题辨析力的鉴定结果	2	5	1	0	0	60%
		时事政策水平综合测试成绩	1	6	1	0	0	40%
	事业心 30%	对岗位认知、扎根基层、建功立业等方面测评结果	0	1	7	0	0	35%
		毕业分配态度鉴定结果	0	3	5	0	0	65%
	守纪用法 20%	遵纪守法情况鉴定结果	2	5	1	0	0	55%
		运用法规处理问题鉴定结果	2	4	2	0	0	45%
	基层政治工作 30%	思想工作	1	3	4	0	0	30%
		组织工作	2	4	2	0	0	30%
		宣传工作	1	4	2	1	0	20%
		文化工作	0	3	4	1	0	20%
任职基础素质 30%	军官素养 35%	决断力	1	5	1	1	0	30%
		示范力	1	4	2	1	0	30%
		感召力	1	5	1	1	0	40%
	专业技能综合应用 30%	专业技能综合应用测试成绩	2	4	1	1	0	100%
	信息素质 15%	网络技术	1	3	2	2	0	45%
		数据处理技术	0	3	3	2	0	55%
	身体素质 20%	体能考核成绩与体格检查结果	3	4	1	0	0	100%
岗位业务素质 50%	指挥作战 30%	综合演习（演练）考核成绩	2	5	1	0	0	100%
	组织训练 30%	“四会”教练员考核成绩	1	6	1	0	0	100%
	领导管理 20%	在模拟连任职考核成绩	1	3	4	0	0	100%
	岗位适应 20%	实习鉴定成绩	2	3	3	0	0	60%
		掌握不同岗位、不同型号装备的数量	1	4	3	0	0	40%

我们以思想政治素质中的“政治鉴别力”素质的综合评判计算为例

(2) 模糊关系矩阵：评审专家 8 人，对某学员评定如表

(1) 因素评价的权数分配如表为 (0.6, 0.4)

评估点	评价等级和评分				
	优秀 100—90	良好 89—80	中等 79—70	及格 69—60	差 59—0
对重大原则问题辨析力的鉴定结果	2	5	1	0	0
时事政策水平综合测试成绩	1	6	1	0	0

3.2.1 “政治鉴别力”的综合评判

模糊关系矩阵

$$B_1 = A_1 \times R_1 = (0.6 \quad 0.4) \times$$
$$\begin{bmatrix} 0.25 & 0.625 & 0.125 & 0 & 0 \\ 0.125 & 0.75 & 0.125 & 0 & 0 \end{bmatrix}$$
$$= (0.2 \quad 0.675 \quad 0.125 \quad 0 \quad 0)$$

同理“事业心”的综合评判，“守纪用法”的综合评判，“基层政治工作”的综合评价 (0 0.2875 0.7125 0 0)，( 0.25 0.56875 0.18125 0 0 )，( 0.1375 0.4375 0.375 0.05 )

3.2.2 二级层次“思想政治素质”的综合评价

$$\underline{B}_1^* = \underline{A}_1^* \circ \begin{bmatrix} \underline{A}_1 \times \underline{R}_1 \\ \underline{A}_2 \times \underline{R}_2 \\ \underline{A}_3 \times \underline{R}_3 \\ \underline{A}_4 \times \underline{R}_4 \end{bmatrix} = (0.2 \quad 0.3 \quad 0.2 \quad 0.3) \times$$
$$\begin{bmatrix} 0.2 & 0.675 & 0.125 & 0 & 0 \\ 0 & 0.2875 & 0.7125 & 0 & 0 \\ 0.25 & 0.56875 & 0.18125 & 0 & 0 \\ 0.1375 & 0.4375 & 0.375 & 0.05 & 0 \end{bmatrix}$$
$$= (0.13125 \quad 0.46625 \quad 0.3875 \quad 0.0150 \quad 0)$$

同理得二级层次“任职基础素质”的综合评价和二级层次“岗位业务素质”的综合评判为 ( 0.230625 0.51375 0.155625 0.1 0 )，(0.1775 0.5725 0.25 0 0)

3.2.3 三级层次“学院综合素质”的综合评判

1)  $\underline{A}^*=[$ 思想政治素质，任职基础素质，岗位业务素质] $= (0.2 \quad 0.3 \quad 0.5)$

2) 
$$\underline{B}^* = \underline{A}^* \times \begin{bmatrix} \underline{B}_1^* \\ \underline{B}_2^* \\ \underline{B}_3^* \end{bmatrix} = (0.2 \quad 0.3 \quad 0.5) \times$$
$$\begin{bmatrix} 0.13125 & 0.46625 & 0.3875 & 0.015 & 0 \\ 0.230625 & 0.51375 & 0.155625 & 0.1 & 0 \\ 0.1775 & 0.5725 & 0.25 & 0 & 0 \end{bmatrix}$$
$$= (0.1842 \quad 0.5336 \quad 0.2492 \quad 0.033 \quad 0)$$

3.2.4 计算  $\underline{B}^*$  的综合评价

$$W = \underline{B}^* \times C^T = (0.1842 \quad 0.5336 \quad 0.2492 \quad 0.033 \quad 0) \begin{bmatrix} 95 \\ 85 \\ 75 \\ 65 \\ 45 \end{bmatrix} = 83.69 \text{ 分}$$

某学员的综合素质经综合评价获得 83.69 分，因此该学员的综合素质属于“良好”类型，与实际吻合。

3.3 模糊综合评判的特点

通过建立“多层次、多算子的模糊数学模型”用于多因素的综合评价，是对人们决策思维过程的数学描述。

连排级指挥军官任职教育学员素质是多因素的，划分为“思想政治素质、任职基础素质、岗位业务素质”三个方面，十二个类别、二十二个项目，属于较复杂的系统，形成一种现代化科学评价人才的方法。

多层次，多算子二型模糊数学模型综合评价体现了如下优越性：

科学性：通过建立模糊教学模型对任职教育学员的素质进行综合评价，不仅能客观地反映任职教育学员素质的真实情况，而且能使定性描述量化。

可靠性：模糊集合理论和数学模型，在理论体系上是严密的，计算方法和过程是正确的，而且可通过编制程序设计，用计算机给出综合评价的最后

结果。

简易可行性：整个计算步骤明确、判断简便，懂得线性代数就可掌握这种计算方法。

### 参考文献

- [1] 任富兴. 炮兵信息化建设. 北京：解放军出版社，2004 年 10 月第 1 版
- [2] 向德全. 军事教育评价概论. 西安：西北大学出版社，2006 年 10 月
- [3] 张连盈. 军校教育评估. 北京：解放军出版社，2006 年 10 月

### 作者联系方式

通信地址：炮兵学院南京分院侦察教研室

邮政编码：211132

联系电话：025-80810819

# 关于军队信息化人才培养的思考

司维超 李连 王文才

摘要：论述了信息化人才的重要性，分析了我军目前在人才培养方面的现状及不足，给出了几点信息化人才培养的对策。

关键词：信息化；信息技术；信息化人才；人才培养

20 世纪中后期以来，随着信息技术的发展，人类历史上首次拉开了第四次科学技术革命的帷幕——信息技术革命。随之产生的以信息技术为标志的新军事变革便成为当今军事领域的最显著特征。21 世纪，人类已步入信息时代，战争形态正由机械化向信息化转变，夺取信息优势成为作战的重心。信息技术的飞速发展及多元化使新军事变革出现跨越式的发展。

## 1 信息化人才在军事信息化中的重要性

通过各国的军事信息化建设比较，我们可以看出，它具有“广”、“化”、“难”的特点，即涉及领域广、持续时间长、发展建设难，并且影响因素也千变万化，但其中最主要同时也是制约信息化发展的“瓶颈”却是人才的匮乏和整体素质不高。加大力度培养信息化人才已经成为各个国家进行信息化建设的重中之重。

信息化人才与军事信息化相辅相成。军事信息化是信息化在军事方面的发展，而人才建设能带动信息化建设，信息化建设又能促进部队信息化的全面发展，所以培养信息化人才必定能推动军事信息化的发展。从另一个角度来看，军事的信息化其中一个重要的方面就是培养信息化人才，以此来说，它们是充分的关系；由前一步培养出来的信息化人才，经过理论创新、技术钻研又可以促进军事信息化的进一步发展，以此来说，它们是必要的关系。如图 1 所示。

信息化人才是赢得战争的关键因素。未来战争是信息化的战争，交战双方谁能更好的全程获取、高效处理和充分利用信息，谁就能赢得战争的“制信息权”，从而最终获得战争的胜利。但是，再现

代的作战理论、再先进的武器装备，离开人的主导，也只不过是“废铜烂铁”。另外，单单有了人还远远不够，我们需要的是信息化人才，是能掌握并利用信息技术为军队做贡献的“人”。这就涉及到如何将普通人培养成为信息化人才的问题。

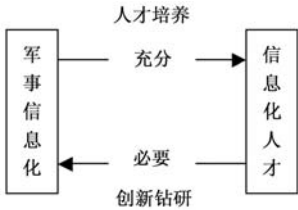


图 1

## 2 目前我军信息化人才现状及不足

随着军事信息化的不断发展，基层信息化人才力量相对不足，人才培养工作相对薄弱的问题日益突出。与社会生产力的发展、信息技术的不断更新、水平需求日益高的信息化工作相比，信息化人才素质低、质量差、数量少、培养不足，已经成为当前人才培养工作中不可忽视的问题。

1) 信息化人才得不到充分的重视。虽然，现在信息化建设已深入人心，但不乏部分领导对信息化认识不到位，或是心里明白，但一结合实际就变了味。导致长期以来，形成了“重业务、轻信息化”的问题，信息化人才得不到重视，出现大材小用及人才流失的现象，严重阻碍了信息化的发展。

2) 信息化人才数量少、素质低。虽然，我们每年毕业或轮训的学员不少，但真正属于信息化人才的仅占少数，基层中大部分所谓的“信息化人才”，大都半路出家，或由懂得一点电脑知识的人担任，整体上缺乏信息化理论基础。工作上，缺乏利用信息化知识进行再创造的能力，大都按部就

班,破坏了军事信息化与信息化人才之间的充分必要关系。另外,信息化人才的缺乏,往往会导致“一人兼多职”的现象发生,这样虽然从表面上看,各项工作都有了进展,但实际上是属于“眉毛胡子一把抓”,分散了人员的精力,使他们无法全身心的投入到信息化建设中去。

3) 信息化人才培养不足。现在是信息时代,同样也是知识大爆炸的时代,新知识、新技术呈现出种类花样多、更替周期短的特点。这便从两方面对我们提出了要求:增加信息化人才的数量;加大信息化人才的再培养力度。而目前我们无法很好的做到信息化人才的“实时更新”,即使有也是“阶段更新”,所以,很难适应部队信息化的发展需要。

4) 信息化人才引入较难。除了我们部队自产自销外,还应该遵循“走出去,引进来”的策略,充分利用社会资源,引入高水平信息化人才。这样一来,我们就面临很多问题:一是待遇问题。目前来说,信息化人才是很缺乏的,在这个比较现实的社会里,一边是条件优厚的外资企业,一边是相对比较艰苦的部队,除了有报国之心之有识之士外,很多人还是会选择前者的;二是录取考核问题。考试制度目前来说还是主流的检验方式,仅仅从几份试卷或几个题目是无法充分定位某一个人是否真正具有信息化水平的,这样选拔出来的人才,往往无法真正适应部队信息化建设需要。

### 3 信息化人才培养的几点对策

#### 3.1 从大局着手,做好人才培养顶层设计

进行军事信息化要有明确的目标,必须从总体上进行规划设计,而作为其中的关键即信息化人才的培养更要做好长远规划,既要跟得上时代潮流,又要能体现出我军特色。

一是要对比发达国家信息化人才培养战略,取长补短,为我所用。历史教训表明,“闭关锁国”只会导致国家越来越落后,我们不能过高的估计自己的实力,也不可觉得自己一无是处,要细心研究国外发达国家的先进的理念及策略,查找自身不足,为制定出信息化人才培养战略指明方向。

二是要摆脱传统思想的禁锢,树立信息化人才建设新观念,做好人才培养顶层设计。旧思想旧传

统虽然有值得我们学习借鉴的地方,但在新形势下,要做好新型人才的培养,必须首先使设计者的思想得以解脱,顺应时代的发展,建立人才建设新观念。树立全面协同观念,军事信息化人才的培养不能仅仅依靠部队一己之力,而是要集社会之长,实行军地合作,全面协同的模式;超前发展观念,俗话说“书到用时方恨少”,真正等到我们迫在眉睫需要人才时才开始考虑培养人才,那样不但因为时间仓促而使人才质量大打折扣,而且即使人才出炉后,对应的武器装备也可能会不再先进,所以要杜绝“装备等人才”现象发生,打好人才培养的提前量;稳步发展观念,人才的培养是一个长期积累的过程,切忌急功近利,搞“大跃进”,要扎实做好每一步,为人才的“大厦”打下稳固的基础;高效费比观念,在信息化飞速发展的今天,坚持效益之上的原则,集中力量办大事,做到花费最少的代价,培养出高效率的人才。

#### 3.2 从具体着手,健全人才培养科学运行机制

针对人才培养的具体每一步,都要认真思考,深入探究,制定出一条科学的运行机制。

##### 3.2.1 创新运用“院校集中培训,训练基地集中轮训”的人才培养主渠道

目前,实行“院校集中培训、训练基地集中轮训”仍就是我们军队培养人才的主要方式。但是不能按部就班,走老套路,要随时代发展而变化,吸收新的培养方式。

首先,院校培养是人才培养的第一步,以往的培养机制无法完全适应新形势下的人才培养需求,必须要在原有基础上进行创新。

1) 提高师生信息素养。以往评价教学员素质高低,只不过从为人处事、学术水平等方面进行比较,现在这些远远不够,要将信息化素质高低列入日程。要针对信息化开展专门的教与学活动,比如开展信息化学习月、知识竞赛等。在思想上教育大家,可以从三方面着手:一是开展信息化研讨会、专题报告等形式,从总体上进行引导;二是在教学过程中,教员要将信息化知识充分融合到课程讲解当中,时刻突出信息化重要性;三是鼓励学员围绕信息化展开激烈讨论,得出自己的心得。

2) 改革应试教育模式。传统的应试教育长期



以来，始终以考试的方式对学员的学习效果，教员的授课水平进行检验，虽然达到了一定效果，但在更大程度上却使学员形成了“学习为考试”的观念。如今的现状，要求我们必须对应试教育进行改革。首先，对教学方式进行了改革，避免满堂灌的方式，要转变为以教员引导为辅，学员自学为主的方式。鼓励教员积极探寻创新教学及转变学员学习动力的方法，使他们真正学到知识。加强教学员互动和双向交流，及时掌握现状，对教学进行适时调整。建立信息化教学试点，为信息化的进一步普及积累经验；其次，对考核制度进行适当改革，将重心从考试转移到全方面检验，考试成绩只作为检验标准之一，还要对学员的动手能力、创新能力等进行考核，最终是以综合成绩来评价学员的学习成果的。并由此成绩建立学员综合能力一览表，反馈给教学部门，分门别类针对学员的弱项在下一步的教学中加强培养。

3) 教学内容上要创新，加快学科体系的信息化改造。首先，在信息知识大爆炸的情况下，单纯的教授新知识，已经不能满足信息化的需要，必须要在教学内容上进行改革。要由以教授知识转变为教授独立学习方法，教授如何利用信息化技术，要突出信息化课程，并实时更新内容；其次，利用现代信息技术加快对优势学科进行信息化改造，努力发展边缘交叉学科以及人文学科。

4) 教学管理上要创新。军校的管理，向来以“整齐划一”为宗旨。在这种模式下，学员的个性往往被看作是不合群的标志，受到了严格的管制；

他们的一些新奇的想法，也被视为胡思乱想，个性张扬。这样培养出来的人才，毫无个性可言，因循守旧是他们的本领，缺乏创新是他们的特点，离信息化人才相差甚远。因此，我们要对管理上的不足进行改进。首先，在严格管理的前提下，适当培养学员的一些积极的个性，使他们意识到在遵守纪律的前提下，个性是可以发挥的；其次，采取措施，如兴趣小组、第二课堂等形式引导学员发挥特长，培养创新性，并予以鼓励表扬；再次，加强人性化管理，采取学员自治方式，提供学员参与教学管理的机会，培养学员综合素质。

其次，基地集中轮训是院校培训的深入，属于人才的再培养。

在人才培养上实现院校、基地的互相交流合作。通过交流合作，共同摸索出一条人才培养及再培养的机制。院校通过跟踪人才的部队实践，发现规律及存在的缺陷，为以后培养查缺补漏；部队则通过将人才送往院校进行深造，不断提高人才信息化水平，为以后自身的信息化建设做好准备。

利用软件工程的观点，对信息化人才的培养进行模块化。由于部队各单位情况各异，信息化建设也参差不齐，基地集中统一培训，往往造成资源的浪费。在这种情况下，可以将信息化培训内容分为一些独立的模块，各单位待培训人员则根据本单位实际情况，进行针对性的学习，节约成本，提高效率。另外，随着信息化的发展，还可以在每个单位实现远程培训，网络教学及网上交流等方便快捷的手段。如图 2 所示。

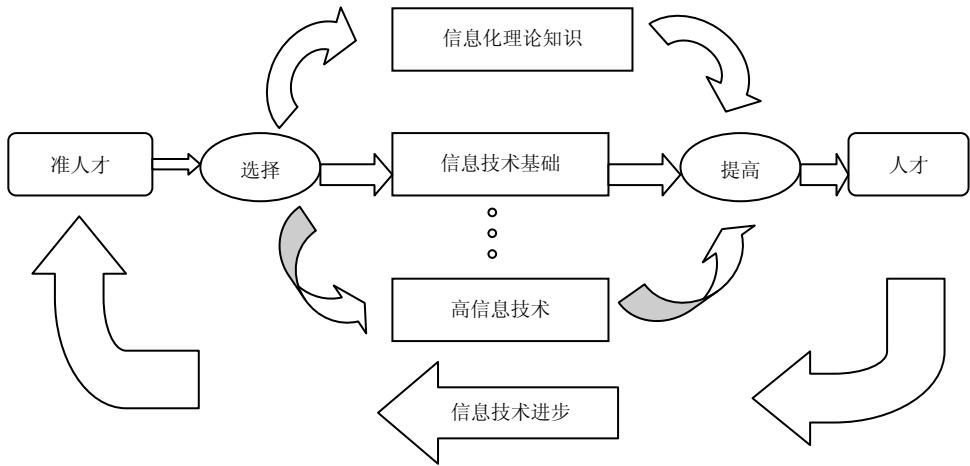


图 2

### 3.2.2 “走出去，引进来”，搞好国内外、军内外人才培养互通、互联、互合作

这里所说的“走出去，引进来”有两方面的涵义：一是走出国门，走向世界，引进发达国家先进的人才培养机制；二是走出部队，走向社会，引进社会资源及人才。

走向世界。组织专门的研究人员，时刻关注外军的信息化建设，比较他们针对人才培养问题所采取的方法，查找其优缺点。针对其优点可以进行借鉴，转变为适合我军特色的途径；对其缺点及经验教训，反查自身问题，及时采取对策，亡羊补牢。选拔部分信息化人才到国外进行深造，掌握先进的信息技术和人才培养理念；邀请外军来我军进行参观，大力宣传我军信息化建设水平。

走向社会。前文也提过单靠部队一己之力，很难完成人才的全面培养，要充分利用社会资源，实行军地合作培养，建立诸多共建单位，将部队的人才送往社会，比如地方大学、科研单位企业等进行代培训，这样既可以使他们了解到信息技术的广泛用途，又学到了新知识。同时也可以利用这样的机会对部队进行大力宣传，鼓励更多有报国热情地学

子参与到部队信息化建设当中来；加强军地资源共享，人才交流。部队资源总是有限的，分配到具体的某个单位更是很少，因此要借助社会上的丰富资源，比如地方大学的师资力量，先进的信息技术等，创新的融入到部队信息化建设中来。邀请地方信息化人才到部队做演讲报告，不断提高官兵的信息化素养，了解信息技术发展最新动态，让部队信息技术人才走出去，协助地方开展信息战等方面的教学，不断提高国民的信息素养。经常性组织人才的交流研讨会，提出问题，并讨论解决，共同提高信息化水平。

## 4 结束语

信息化的脚步不会停止，新军事变革还远未结束。我们与世界强国的差距是客观存在的，在这种环境下，我们要正确认识当前形势，戒骄戒躁，杜绝急功近利，加快培养信息化人才，为信息化的进一步发展提供新鲜血液。

### 参考文献

- [1] 陈辉.打赢信息化战争 中央军委颁发军队人才战略规划.新华网
- [2] 赵丕.浅析外军信息化作战与建设实.外国军事学术.2006年第8期
- [3] 王保存.各国军队信息化建设的不平衡性.学习时报.2004年
- [4] 廖作斌.军事信息人才的培养.学习时报.2004年
- [5] 张建昌.推进我军信息化建设的思考.解放军报.2003年01月28日 第6版

### 作者联系方式

通信地址：山东烟台市二马路188号304教研室

邮政编码：264001

联系电话：0535-6635690

# 浅谈信息化参谋人才的培养

王海源 辛文军 赵东方

**摘 要:** 本文从信息化参谋人才的能力要求, 培养机制建设等方面简要阐述了信息化参谋人才培养的相关问题, 对提高信息化参谋人才培养有着深刻的思考。

**关键词:** 信息化; 参谋人才; 培养

当今世界, 以信息技术为核心和基础的新技术革命蓬勃发展, 正以排山倒海之势冲击着现代社会生活的各个领域, 使人类社会由工业时代迈向信息时代。在军事领域, 新技术革命推动了新军事革命的兴起, 促使信息战时代的到来, 信息战已成为高技术局部战争的主要作战样式。为迎接信息时代和信息战, 为加强我军司令部信息化建设, 迫切需要一批高素质的信息化参谋人才。

## 1 信息化参谋人才培养目标

信息战环境下, 参谋人员必须适应未来变幻不定的信息战需要, 能够组织收集、处理和传输信息情报夺取、掌握和利用信息优势, 协助指挥员定下正确决心。近年来, 我们在培养高素质参谋人才方面下了很大的功夫, 取得了一些成绩, 但是也存在一些问题。主要是针对性不强、信息技术含量不高。因此, 培养信息战参谋人才必须要有所侧重, 使他们具备信息获取与处理能力, 运筹与谋划能力和组织与控制能力。

### 1.1 信息获取与处理能力

未来信息战中, 各种信息情报弥漫整个战场, 有有用的也有无用的, 有价值高的也有价值低的, 信息战参谋人才必须要有较强的辨别力, 从纷繁的信息中筛选出有价值的信息为己所用, 准确及时地掌握各种作战情况特别是敌方情况, 以确保组织指挥建立在符合战场实际的基础之上。

### 1.2 运筹与谋划能力

信息战参谋人才必须着眼作战全局的需要, 根据已获得的可靠信息, 因敌、因地、因时制宜地出

谋划策, 提出切实可行的行动方案。在进行运筹谋划时, 还要运用信息技术手段, 科学选择多种运筹方法和思维方式, 提高运筹谋划的准确性, 以确保指挥员所定下的决心是建立在客观、可行的基础之上。

### 1.3 组织与控制能力

在信息化战争中, 参战军、兵种多, 建制单位多, 支援保障量大, 敌我双方战线模糊, 作战样式转换频率高、速度快, 部队流动性大, 计划组织工作和协调控制工作的地位更加突出。信息战参谋人才必须发挥信息优势, 实时监控战场动态, 适时督导并协调各部队的行动, 保证首长决心的圆满完成。

## 2 信息化参谋人才培养对策

### 2.1 制定既科学又实用的人才培养规划

要从信息化发展的特点和部队建设的实际需要出发, 制定既科学又实用的参谋人才培养规划, 否则就欲速则不达。当前在信息化参谋人才培养上存在盲目培养的问题, 有的单位没有思考本单位任务特点和专业实际, 需要什么样的参谋人才, 培养的人才下一步要发挥什么作用, 而是误认为把一些学历高或有某些特长的人员吸收进入信息化参谋人才的培养行列, 就是信息化建设的需要。从而造成了很多被吸收的人才因无用武之地而荒废。因此, 在培养信息化参谋人才时, 应先分析各种人才在现有条件下的具体作用, 以及这些人才的发展方向, 站在部队建设和个人发展的两方面来思考问题, 只有这样, 才会使引进的人才真正为部队建设发挥作用。同时, 还应根据本部队对人才的需求和编制体

制的实际,制订人才引进规划和标准,把好引进人才的质量关。

## 2.2 建立“军地联手,院校培训,实践锻炼”培养机制

根据我国国情、军情,信息战参谋人才在培养机制上,应本着“军地联手、院校培训、实践锻炼”的原则,不断提高参谋人员的信息战能力。

### 2.2.1 军地联手,优势互补合力育才

信息时代,信息化武器系统的信息技术具有军用和民用双重性质,信息技术的这种双重性,为军民结合培养信息作战人才提供了客观可能性。

从现职参谋人员中选拔有一定基础的优秀人才,送入地方理工类大学进行信息知识的学习;从地方计算机、信息自动化等专业大学毕业生中选拔优秀学生入伍,到军事院校进行参谋专业学习;选拔优秀参谋人员到军队电子、信息工程类院校深造,等等,充分挖掘军地院校的潜力,进行联合培养。

### 2.2.2 院校培训,增加信息战课程比重

随着信息武器的不断发展,信息战理论也不断变化,各级指挥院校的高科技教学要进一步充实和拓宽,增加有关信息作战理论特别是司令部机关的组织指挥理论的教学,提高参谋人员的信息战水平,达到既能指挥谋划又具备信息战技能的专家型指挥参谋人才。

### 2.2.3 实践锻炼,在训练中提高信息战能力

建立实验室、训练基地、科研院所、试验部队实践锻炼机制,利用现有资源广泛开展信息战理论的研究和训练演习,组织参谋人员到有关部位参观学习,到信息化建设突出的部队司令部机关代职或培训,积极参与部队信息化训练和演习。努力开发训练模拟系统和信息化作战仿真实验室,采用先进

的科学技术手段,培养司令部信息战参谋人才的信息战能力。还可以通过与地方高等院校、科研院所和信息产业部门进行合作研究,在研究攻克信息战技术和指挥难题的过程中,使军队干部得到锻炼与提高。还应当把扩大对外开放,增进国际学术交流,作为培养信息战人才的重要途径。充分利用我国对外开放的大好时机,通过多种途径、多种方式,加强与外军的交流与合作。既可以派遣参谋人员出国留学、进修、讲学、进行学术研究,参观外军信息设施,参加联合演习,也可以聘请外军信息作战的专家到我军讲学,开阔参谋人员视野和思路,提高自身的信息作战能力。

## 2.3 建立“优胜劣汰”考评激励机制

严格落实“优胜劣汰”的考评激励制度。彻底克服“干与不干一个样,能力好与差一个样”的不良倾向影响信息化参谋人才培养效果,坚持开展争当“优秀参谋”、争创“精武标兵”等活动,并建立工作业绩考评排行制度,实行末位淘汰制,做到能者上,不能者下,形成争先创优的良好氛围。严格落实领导责任制。受训者的考核成绩与个人年度考核成绩和单位训练成绩挂钩,作为单位领导年终评功、评奖和调职晋衔的主要依据考虑。从而激发参训人员训练的积极性和自觉性。

总之,信息化参谋人才不是天生的,是要靠各级领导一步步,一点点发现和培养出来的。在当前军队信息化建设处于快速发展,高技术装备陆续装备部队的情况下,培养一支掌握信息化作战技能的参谋人才队伍已是一个不可忽视的战略问题,也是抢占打赢先机的可靠保证。只有那些着眼部队长远建设,重实际重实效的部队领导,才会注重从打基础入手,一步步地实现培养一支强有力的信息化参谋人才队伍的目标。

## 参考文献

- [1] 《21世纪信息化战争理论研究》.李小军等.北京:军事科学出版社,2000
- [2] 《信息化条件下联合作战工程保障理论研究》.苏怀东等.北京:长征出版社,2006

## 作者联系方式

通信地址:江苏省徐州市工程兵指挥学院桥梁渡河教研室

邮政编码:221004

联系电话:0516-83150714 13605211840

# 信息化人才信息素质的培养

吴楠 毕梅冬

**摘 要:** 本文通过分析信息素质的内涵, 借鉴国外信息素质教育的成功经验, 结合教学实践, 探讨了院校开展信息素质教育的措施和途径, 以期推动、促进信息化条件下军事人才的信息素质的培养。

**关键词:** 信息化人才培养; 信息素质; 院校教育

## 1 引言

当前我军正处于完成机械化、信息化建设双重使命, 解决打得赢、不变质两大课题, 实现国防和军队现代化建设“三步走”战略目标的关键时期。在机械化战争向信息化战争的发展进程中, 无论是火力战、封锁战、特种作战、一体化联合作战, 还是电子战、信息战、网电一体战, 都需要军事人才具备相应的信息素质, 但目前部队信息素质的现状与这种要求之间存在着较大的差距。信息意识淡薄, 信息安全意识和知识缺乏, 信息能力不高的现象还比较普遍, 影响了信息技术装备作用的发挥, 也在一定程度上影响了军事斗争准备工作的开展。因此, 军校加强信息素质教育, 研究军事人才信息素质是如何构成的? 军校如何培养学员的军事信息素质? 这些都是摆在军事教育工作者面前的迫切问题。

有信息素质的人, 他必须能够确定何时需要信息, 并已具有检索、评价和有效使用所需信息的能力”。1992年美国学者 Doyle 在《信息素质全美论坛的终结报告》中给信息素质下的定义是: 一个具有信息素质的人, 他能够认识到精确的和完整的信息是做出合理决策的基础, 确定对信息的需求, 形成基于信息需求的问题, 确定潜在的信息源, 制定成功的检索方式, 从包括基于计算机的和其他的信息源获取信息, 评价信息, 组织信息用于实际的应用, 将新信息与原有的知识体系进行融合以及在批判性思考和问题解决的过程中使用信息。

信息素质包涵诸多方面: ① 传统文化素养的延续和拓展; ② 使受教育者达到独立自学及终生学习的水平; ③ 对信息源及信息工具的了解及运用; ④ 必须拥有各种信息技能: 如对需求的了解及确认; 对所需文献或信息的确定、信息检索; 对检索到的信息进行评估、信息组织及处理并做出决策。综上所述, 信息素养至少应包括三个层面: 文化素养(知识层面)、信息意识(意识层面)以及信息技能(技术层面)。

## 2 信息素质的内涵

### 2.1 信息素质构成要素

信息素质概念的提出, 是一个不断完善的发展过程。“信息素质”一词最早是由美国信息产业协会主席 Paul Zurkowski 在 1974 年给美国政府的报告中提出来的。他认为信息素质是人们在工作中运用信息、学习信息技术、利用信息解决问题的能力。1987 年, 信息家 Patricia Breivik 将信息素质概括为一种了解提供信息的系统并能鉴别信息的价值、选择获取信息的最佳渠道、掌握获取和存储信息的基本技能。1989 年美国图书馆协会下属的“信息素质总统委员会”把信息素质定义为“要成为一个

### 2.2 军事人才必备的信息素质

军事人才的信息素质是多种能力和素质结合在一起的一种素质。

#### 2.2.1 军事人才必备的知识层面的信息素质

① 信息知识。军事人才应当掌握的信息知识主要有: 信息技术的基本常识与历史、信息系统的工作原理、信息系统的结构与组成、信息技术的作用和影响等。② 信息安全知识。军事人才应当具备的信息安全知识包括: 了解信息资源安全的内容, 知道对信息资源安全的威胁和确保信息安全可

以采取的技术、管理措施。③ 信息战知识。军事人才应当具备的信息战知识包括：了解信息战的定义及实质，明确信息战的原则和信息作战的构成要素，了解各种信息战的主要用途和作战目的等。

### 2.2.2 对现代军事人才必备的意识层面的信息素质

① 信息意识。军事人才的信息意识包括：坚定信息制胜观念、强烈而明确的信息需求和较高的信息敏感性。② 信息安全意识。军事人才的信息安全意识是军事人才对信息安全的认识和观念的统称。它包括3个方面：信息安全关系国家安全的观念、信息安全法规意识和信息安全人人有责的观念。③ 信息道德意识。军事人才的信息道德是军事人才在使用信息和信息系统时，应该遵守的行为准则和规范的总称。军事人才的信息道德意识主要体现在，能够正确认识信息技术的作用，具有高度的社会责任感和良好的网上军人形象等方面。

### 2.2.3 对现代军事人才必备的能力层面的信息素质

① 信息系统使用能力。信息系统的使用能力范围十分广泛，包括能不能正确无误地操作信息处理系统；能不能根据工作需要选择合适的软件并正确、熟练地使用；能不能使用军事网络系统完成网上模拟作战指挥作业，能不能熟练使用数字化战场的各种信息设备等。② 信息能力。信息能力是指以各种形式发现、评价、利用和交流信息的能力。军事人才的信息能力包括：信息获取能力、信息理解能力、信息处理能力、信息利用能力、信息创造能力。③ 信息战能力。现代军事人才的信息战能力包括信息战组织能力、信息战防御能力和信息抗干扰能力。

## 3 信息化条件下院校信息素质教育的实施

### 3.1 适应军事斗争的要求，以先进的理念为指导，优化信息化教学设计。

提高军事人材素质，实施并打赢信息战是我们建设信息化军队的根本出发点和归宿点，军校信息素质教育是未来军事斗争对军校人才培养提出的新

要求，是院校提高培养对象信息思维和信息行为的一种新的教育理念和模式，它是素质教育的深化和发展，是终身学习的基础，适用于各种学科、学习环境、学习对象和教育形式，是军事教育现代化的必然趋势，是培养创新军事人才的重要途径。要明确信息素质对军事人才的重要性，把信息素质作为现代军事人才整体素质的一个重要方面，放在军事人才全面素质的大系统中进行研究。

社会信息化的发展对军事教育产生了巨大的影响，使教育体制、教育理念、教学内容、教学模式、教学方法和教学评价发生了改变。信息化社会改变了学习者的学习行为，学习不是一个信息积累的过程，而成为信息处理的过程，学习者不是信息的接受者，而是信息的处理者。更加明确以学员为主体的教育模式，出现了过程性学习、研究性学习、资源型学习和协作型学习等多元学习方式。

信息化教学设计首先要根据学员信息素质现状，培养目标和学员发展来确定信息化教学内容及标准，制定不同教学对象的信息素质课程学习计划，分层次教学，课程目标逐渐提高，采取灵活多样的教学策略，以学生的兴趣和爱好、需求、能力和态度为基础编制课程教材，注意因材施教，争取学习目标和行为目标的一致。

信息化教学设计注重学习资源的充分利用以及开放式、启发式、实验式、案例式教学过程的设计，注意问题导向、资源导向，更加体现以学员为主体的研究式、协作式的学习思想。利用信息技术促进教学，利用网络资源支持教学，使教员更好地肩负信息素质教育者的使命与职责。

### 3.2 注重教员信息素质的提高，为信息素质教育的实施提供必要条件

教育部《关于推进教员教育信息化建设的意见》，对于全面提高教员队伍的信息素质提出了具体要求，教员在信息化教育中的作用没有减弱，反而更加重要。教员必须适应信息化对教学的新要求提高信息素质和教育能力，这是实施信息素质教育培养高素质军事人才的必要条件。

教员具有良好的职业道德与素质、较强的专业知识和外语水平之外还应具备信息方面有关的广博知识，具备跟踪最新信息知识、掌握新信息技术应用的能力。除信息技术学科教员和教育技术工作教员的信息素质主要包括：信息基础知识，信息意识

和信息伦理道德,信息能力,信息教育和科研能力。信息教育和科研能力是教员在教育教学中应用信息技术、利用信息资源培养学员的信息素质、提高教育教学质量和开展相应的科研活动,并具备通过信息工具进行继续学习和发展的能力,信息化教学设计是教员信息教育与科研能力的核心。

通过建立在职教员培训和新教员岗前信息技术培训制度,开设信息技术课程和各种信息知识讲座,培养教员良好的信息素质和利用信息技术的意识和能力,促进信息技术与学科课程的整合。培训教育可分3个层次:一、初级班,主要是进行入门教育,以互动式的课件自学为主;二、中级班,在初级班的基础上培养发现、评价、利用信息的能力;三、高级班,培养把信息技能应用到学科课程中去。学习信息技术基本知识、基本原理,掌握信息搜集、分析、加工、利用的基本方法,掌握教学软件的开发设计与网络教学的基本技能,教育技术与课程的整合能力等,掌握以信息技术为基础的教育技术,通过培训并建立有效的约束激励机制,提高教员的信息素质作为教员必备的职业技能。加强教员信息道德教育,能够对信息进行正确的判断和选择,用信息道德标准规范自身的道德行为与活动,从而为信息素质教育的实施提供必要条件。

### 3.3 注重信息技术与学科教学相结合,提高军事人才信息意识、道德和信息应用能力

#### 3.3.1 信息技术与学科教学相结合

信息素质教育的具体实施表现为信息技术与学科课程的整合,包括教育与学习理念的整合、教学对象与内容的整合、教学方法和手段的整合、教材的整合、教学媒体的整合等。借助现代信息技术特别是多媒体和网络通信技术提供的学习环境,实现自主、开放式全新的学习模式。把信息技术作为处理信息的工具、问题解决的工具和交流协作和决策的工具。排除单纯的信息技术理论教学,而应该关注信息技术的工具论和文化论的有机融合,强调信息技术的应用,以及与实践的联系。适应信息素质教育的需要,合理设置相关课程,将信息技术应用与学科课程的教学结合起来,将信息素质教育融于整个教学过程,根据信息社会发展的需要以及与现实军事实践的联系,根据当前军事变革的发展及军事斗争需要来学习信息技术,而非孤立地学习信息技术,单独地讲授信息技术,在学科教学中培养学

员信息素质。

#### 3.3.2 军事人才信息应用能力要求

通过信息素质教育,使学员了解信息的产生、组织与传递过程。熟悉所在军事学科领域的不同类型(图书、期刊、数据库等)不同层次(零次、一次、二次和三次信息)的主要信息源,通过分析信息需求确定所需信息的性质、学科范围、时间跨度、语种、学科技能、费用等,了解常用信息检索系统的检索结果类型(全文、文摘还是题录)与信息记录格式,了解网络搜索引擎与图书馆信息检索系统检索的异同。

能够组织与实施有效的检索策略。掌握网络搜索引擎常用的检索技巧,正确使用信息检索系统提供的检索功能,能够根据查全率或查准率评价检索结果、检索策略。关注常用的信息源与信息检索系统的变化,能够使用各种新知通报服务,订阅电子邮件服务和加入网络讨论组。

有效地管理、组织与交流信息。通过信息管理系统对信息进行管理组织,选择恰当形式(学术报告、小组讨论等)、手段(幻灯片、网站、网络论坛等)进行口头、书面表述与交流。

运用批判性思维,构建新的知识体系。制定任务计划,确定任务所需的信息,获得信息并形成总结报告、学术论文、项目汇报、专题报告等,运用批判性思维比较、分析、综合同一主题所检索到的不同观点信息,辨认信息中存在的偏差,在借鉴他人成果的基础上形成新信息,构建自己新的知识体系。

#### 3.3.3 提高军事人才信息意识、道德

信息素质教育不等同于信息技术教育,随着互联网的发展,信息道德、知识产权、网络伦理与信息行为、网络文化和信息安全等问题日益突出,面对日益复杂的现实和虚拟信息环境,加强信息意识和信息道德教育,使学员能够合理、合法地检索和利用信息,了解言论自由的限度,了解知识产权与版权的基本知识,遵循在获得、存储、交流、利用信息过程中的法律和道德规范,不非法使用、损害信息源,正确引用他人的思想与成果,合法使用有版权的文献,用信息伦理和道德准则来规范信息活动行为,这是信息素质教育的重要组成部分。

### 3.4 建立信息素质教育评价体系

美国的信息素质教育一直走在世界前列,美国大学与研究图书馆协会制定的“高等教育信息素质教育标准”,为我们实施信息素质教育提供了评价依据,其主要内容包括以下几个方面。

标准一:学员应具备明确信息需要的内容与范围的能力。具体指标包括:定义与形成信息需要;能够识别多种类型与格式的潜在信息源;知道获取信息的费用以及产生的效益;具备对所需信息内容与范围进行重新评价的能力。

标准二:学员应具备高效获取所需信息的能力。具体指标包括:选择合适的调查方法或信息检索系统,以获取所需信息;构建与实施有效的检索策略;利用联机检索终端或亲自使用一组方法检索所需信息;必要时改进检索策略;获取、记录、管理信息与信息源。

标准三:学员应能客观、审慎地评价信息与信息源,并将其纳入信息库与评价系统。具体指标包括:具有从获取信息中提炼信息主题的能力;为评估信息与信息源形成最初的标准;复合主题概念以形成新的概念;能通过对新旧知识的比较而确定信息的增加值;能确定新的知识对个人的价值体系的影响,并使其融入个人的价值体系中;能通过与个人、领域专家及其他人员的交流,对信息的理解与解释的有效性加以判断;决定是否有必要修订初始的查询。

标准四:学员个人或作为群体的一员能有效地利用信息以完成特定的任务。具体指标包括:能够利用各种可获得的信息完成计划,以及产生特定的信息产品或成果;修订产生信息产品或成果的过程;有效地将信息产品、成果与他人交流。

标准五:了解有关信息使用的经济、法律以及

社会因素,获取与使用信息要符合道德与法律规范。具体指标包括:了解信息与信息技术使用的相关法律、道德伦理以及社会经济问题;在存取、使用信息资源时能够遵守法律、法规、信息资源提供的规定以及约定俗成的一些规则;对引用的成果表示致谢。

美军不仅在国防大学成立了专门培养信息人才的信息资源管理学院,还在所有高等军事院校开设了“信息战课程”和“信息战参谋课程”;不仅培养了大批信息战专家,还使大量军官、士官掌握了信息战基本知识。韩国国防部于1999年初颁布了《2010年信息化军队构想》,制订了“信息战人才培养计划”,并已建立起150个信息化教育场所,计划培养350名信息战高级专家。此外,英、法、日等国军队近年来也加大了培训信息战人才素质的力度。

他山之石,可以攻玉。信息化的发展促使军事教育走向以促进学员全面发展的教育质量评价观,借鉴国外成功经验,建立信息素质教育评价体系,坚持定性评价与定量评价相结合,过程评价与结果评价相结合,制定符合院校实际情况的信息素质教育评价内容和评价标准,强化院校信息素质教育,肩负起培养21世纪创新型军事人才的教育使命。

## 4 结束语

信息化条件下,实施并打赢信息战是我们建设信息化军队的根本出发点和归宿点,面对已经发生和可能发生的信息化战争,适应军事斗争对军校人才培养提出的新要求,军事人才信息素质的培养的提出、研究和开展,都有着十分重要的现实意义。

### 参考文献

- [1] 童天湘.智能社会的形态描述[M].哈尔滨:东北林业大学出版社,1996.
- [2] 韩梅.我国信息素质教育研究综述[J].科技情报开发与经济,2005(5):73-74.
- [3] 王怀诗,李平稳.信息素质教育及其途径[J].图书与情报,2004(1):12-15.

### 作者联系方式

通信地址:青岛海军潜艇学院一系虚拟中心

邮政编码:266071

联系电话:0532-83257351



# 刍议军事院校教学资源优化与共享

杨莉 刘因海 陈振宇

**摘 要：**教学资源是军队信息资源的重要组成部分。本文主要探讨了如何优化军事院校教学资源配置问题，然后从网络建设、资源开发利用和运用信息技术等三个方面提出了教学资源共享信息化的措施。

**关键词：**教学资源；优化与共享；信息化

教学资源是军队信息资源的重要组成部分，因此，军事院校教学资源建设也是我军当前信息化建设的一个不可轻视的重要环节。当前军事院校联合办学顺应了当今世界各国开放办学的大势，其重要性也越来越凸现出来。军校联合办学开展之初，各校都有很高的积极性，可是一旦落到实处问题就出来了，这些问题主要是要解决教学资源优化，实现资源共享。下面就如何实现军校教学资源优化与共享进行探讨。

## 1 做好宏观规划，优化院校整体教学资源配置

### 1.1 界定教学资源的主体内容，研究各院校教学资源的差异

首先联合办学的目标定位要准确。只有准确界定军校联合办学的主体内容，才能实现全方位整体合作。军校教学资源，包括有形资源和无形资源两方面：即有形的人力（师资、教学管理人员等）、财力、物力，比如教室、专用实验室、图书馆、会场、运动馆及其内部包括图书、实验器材以及计算机网络、通讯等系统在内的各类为教学服务的设施、设备器材等；无形的思想、观念、制度等。由于各院校的军兵种性质、所处地理位置、培养层次的不同以及其他因素的影响，形成了各院校的办学特色，因此，它们在教学资源方面存在着较大的差异。这种差异主要体现在不同院校的学科专业设置侧重点不同，课程体系和教学内容也不一样；培养复合型人才要紧紧依托部队，一般是与院校同军兵种或同战区的部队合力育人；每所院校的教学科研设施建设的信息化程度有差别，教学模式和教学效

果也就有区别；不同院校所在的地区军地教育资源以及经济发展程度的不同，这对院校的学科科研水平也有一定的影响。我们要认识到差异，更要充分利用这些差异进行优势互补。

### 1.2 利用组合协同效应，实现教学资源互补

组合协同效应几乎总是通过对资源的充分利用来实现的。在联合办学军校中存在着大量的共同资源以及处于“部分时间工作态”的资源，资源互补首先就是将这些分散的资源联合起来，以取得整体最佳。军校内部的院系是以学科划分来建立的，某个学科的资源其全部效能很可能未被完全利用，或者资源在不同时间的使用强度不同，两个或两个以上学科相互填补空白，从而使多余的资源得以充分的利用。现代学科发展需要交叉融合、多科共进，各个学科都有可能从其他学科研究开发方面付出的努力中，获得直接的或间接的利益。

首先，对于教学思想观念、成熟的规范制度，院校之间应当相互借鉴、吸收、应用。其次，在师资队伍的培训和使用中，可以探索和建立“固定编制”和“流动编制”相结合的教员队伍管理模式与教师资源开发的机制。通过军校联合办学、同一地区军地高校互聘联聘教员、互派访问学者等方式实现教师资源共享。其三，在学员培养上，应积极探索军校联合培养学员的多种模式。应积极创造条件，让不同院校学员能互选部分选修课，互相承认学分，在此基础上，还应探索混合培养人才的新模式。其四，在教学科研保障方面，应探索建立军校共同保障的保障体系。各院校在教学科研保障的内容上差异性较大，但在某些方面仍具有通用性。在一些专业实验室方面军校可互用、共用。一些大型实验设备器材、仿真模拟系统可实行共建共用。图

书等文献资源可通过签订军地高校图书馆通阅协议、图书馆馆际文献传递协议等方式实现共享。

### 1.3 确立协调机制，调节教学资源整合的速度和方向

军校之间有很多共性，但存在也较大差别。这就决定了要实现其教学资源整合必须构建有效协调机制。可以想见，当军校联合办学进一步深入时，将会有更多的问题、矛盾产生。因此多方面原因决定了必须确立一个高效运转的协调机制以组织、指导、调控两者实现联合办学。

首先处理好“循序渐进”与“一步到位”的关系。联合办学的初期，院校间需要经过彼此的了解与磨合。磨合期的长短以及这段经历的剧烈程度，取决于联合办学的性质、类型以及实施过程控制好坏等多种因素。究竟是缓慢过渡，还是快速整合，要在实践中探索。磨合在联合办学中是一个重要的概念，但是又难以操作，用通俗的话来说可以理解为“循序渐进”与“一步到位”的关系处理，或是融合过程中“速”和“度”的把握。

其次，争取做到有法可依，有章可循。共同制订相关配套的法规、规章制度。军校实现联合办学应有相应的法规制度作保证，使合作各方在此问题上有法可依、有章可循，依法促结合。在法规建立上，各方应在统一认识的基础上，着手军校联合办学共育人才的立法工作，用法规的形式将结合工作作为一项长期的制度确定下来。按行政教学管理、教学科研两个序列，各院校内各院、部、系、教研室、研究室等基层单位互建对子，密切合作。

必要时联合办学院校应成立一个常设机构，比如可称为“教育资源共享协调组织”，设立一个秘书处（或别的名称）及秘书长（或别的名称）。其职能主要是协调，负责制定联合办学的规则，消除一些阻碍联合办学的各种规章制度。重在制定规则，消除障碍。有这样一个精干高效的机构，必将大大推进教学资源共享的进程。

## 2 积极创造条件，实现教学资源共享的信息化

信息时代的到来，正以前所未有的渗透作用促使军队各个领域发生深刻的变革。在教育领域，由

于信息中介系统的强烈作用，使知识传播实现了时间和空间的超越，传统教育模式与办学模式受到日益强劲的冲击。着眼提高教学质量和办学效益，军队院校大大加快了现代化信息化教学的进程，这对院校联合办学工作既提出了挑战，更提供了难得的历史机遇。院校联合办学工作如何适应时代发展和教育形势的变化，充分利用现代信息技术，实现跨校教学资源共享，提高协作效益，是当前亟待研究解决的一个问题。

### 2.1 加快网络建设，逐步实现教学资源跨校共享

军校在实现联合办学的过程中，应高度重视信息网络技术在实现两者充分结合中的应用。随着信息网络技术的迅猛发展，各军校陆续建成校园网并与军事综合信息网互联。但由于门户之见等原因，多是封闭式发展，未能充分利用网络技术应用于高素质人才的培养上。当前有必要利用各种网络技术、手段将军校联合起来，实现教学和科研资源、成果共享，共育人才。我们可以采取以下几个方面的措施：一是对校园网及时升级改造，提高网络速率，增大带宽，解决网络传输慢、带宽窄的问题；二是利用军事教育训练网，在现有网站基础上建立跨校共享资源网站；三是加强网络安全保密管理。由于跨校信息资源共享的实现，首先要保证网络信息的安全可靠，因此，我们要运用多种安全保密手段，实现“实体可信、资源可管、行为可控、事件可查、运行可靠”的网络安全防范目标。

### 2.2 重视资源开发利用，建立跨校教学信息系统

在以往的协作中，院校更为注重的是师资、教材、设备、场地等“物”的协作，以达成某种形式的资源共享。随着信息技术的发展和信息应用水平的提高，在协作工作中，优先考虑信息资源的共享，院校协作的主要内容逐步变为“信息”。这种变化，反映了新时期院校需求变化的客观要求。

由于资源种类及数量的增多，数据库检索系统的不同，用户需求不同，因此统一检索平台，一次性用户认证，实现不同系统之间的无缝链接成为提高资源利用率急迫问题。服务手段落后，不仅现有资源不能充分发挥效益，网上的各种“虚拟资源”

也不能为我所用,特别是网上信息资源得不到开发利用,对军校的教学和科研是极大的损失。要想走出困境,就要借助现代化的信息技术手段,共建一个多层次的教学信息服务系统,走共建、共知、共享之路,建立一个开放、高效、整体发展的新型模式,以满足军校教育教学和科研的需要。应当以现代教育思想为指导,以先进实用的技术平台为基础,切实做好规划布局,合理分工,统筹建设教育信息资源体系,避免重复浪费。制定科学的政策措施和运行机制,鼓励和确保资源共享。建设好一批教育软件的资源基地,并鼓励、吸引社会力量共同开发高质量的软件。

## 2.3 灵活应用信息技术,创新跨校教学方式

信息技术本身具有的开放性、客观性、集成性、可控性特征,要求院校之间的协作必须彻底摒弃自我封闭、相互保留的做法,确立公平开放,广泛联合的观念。信息化教学手段的运用,军校中计算机互联网的普及,远程教育手段的广泛运用,尤其是基础课程方面更能充分体现出发挥著名教授、专家和优秀教材的作用,使资源共享成为易于操作和可行性极高的途径。灵活应用信息技术,为联合办学院校开创新的教学模式,表现在将信息技术与教学手段、教学内容和教学管理结合起来。

将信息技术与教学手段的结合,一方面是指学生在学习过程中,可以充分利用信息技术手段,改变学员原来的被动式学习模式,主动地按照自己的兴趣和需求对知识进行快速检索,提高学习效率。同时还将改变理论学习与实践环节脱钩的局限性,通过多媒体技术将现实世界呈现在学员面前,让学员更好地理解知识,提高学员把知识还原成现实应用的能力。另一方面是指教员在教学过程中,要具有且不断提高运用现代信息技术的能力。信息时代的教学理论改变了以教为中心的传统教学模式,教

员将成为学员自主学习的指导者、帮助者和启发者。这需要教员掌握信息化教学设计的方法,努力在工作中应用信息化教学手段,成功地扮演好教学舞台上的新角色;根据自己所教学科的特点,熟悉所教学科内容在互联网上的资源分布情况,以便帮助学员进行研究型、资源型学习;掌握教学评价的新方法,加强信息化环境下的教育科学研究,及时跟踪现代教育技术的发展,应用先进的信息技术改进自己的教学方式和学生的学习方式。

信息技术与教学内容的结合,主要是指的是通过现代信息技术手段,改变传统单一的以文本表示知识的形式,用文字、图像、动画、声音、视频、图形等多媒体的方式,最恰到好处地表现将要传达给学员的知识,模拟仿真战场形势、武器装备,使学员面对知识时犹如身临其境。同时,促进信息技术与教学内容的融合,还将使学员认知知识的方式变得更自然、更人性化,打破传统的文本阅读、文字认知、人工检索的低效束缚。

信息技术与教学管理的结合,指的是教育教学管理工作如何利用信息技术手段,在联合办学院校间建立起顺畅的信息通道,充分调动一切教学资源,为院校的各项业务服务,以提高院校的管理水平和运作效率。通过实现信息技术与院校管理的融合,教育管理者可以利用计算机和网络,依靠对教学资源的整合和实时的交互方式,通过远程教育平台可以为学员进行个性化的服务,并对部分学员进行跟踪,了解他们的学习情况;通过智能的信息收集和办公自动化,可以及时给教员或者学校在教学方面的问题予以指导和帮助;通过培训和考试的方式,进行教员资格的评定,有力地提高教员队伍素质;通过自动的统计功能和决策支持,协助进行教育管理政策、方针的决策,对院校的教学水平进行及时的调控。

## 参考文献

- [1] 汪向东.信息化:中国 21 世纪的选择.北京:社会科学文献出版社.1998 年.
- [2] 中国军事教育,2006-2007.

## 作者联系方式

通信地址:武汉市二七路 145 号二炮指挥学院三系指挥自动化教研室  
 邮政编码:430012  
 联系电话:13397190106 027-85963836

# 以科学发展观为指导，加快信息化条件下军事人才培养

张广忠 仝友谊 赵盼

**摘 要：**本文以探索培养信息化条件下军事人才为目的，从人才培养特点、专业素质以及构建信息化教学体系出发，提出了一些新的观点和看法，希望形成一套完整、合理的培养机制。

**关键词：**信息化；军事人才；培养

随着军队由机械化向信息化转变，信息化建设已成为我军建设的重点。而信息化建设的主体是信息化军事人才，他们素质的高低直接影响到部队信息化建设的顺利实施和战斗力的提高。为了提高部队战斗力，加速建成信息化军队，我军必须以科学发展观为指导，科学培养信息化条件下的军事人才。

## 1 瞄准学科专业前沿，把握信息化条件下军事人才培养特点

军队院校作为培养信息化军事人才的主渠道，必须适应信息化发展的需要。立足当前，着眼发展，瞄准前沿理论，贴近部队作战实际，贴近培养目标的岗位需要，增强整体性，突出针对性。

(1) 瞄准信息化发展的前沿，有针对性地充实教学内容

随着信息时代的到来，人类创造新知识的速率成几何倍率增加，知识更新的周期在不断缩短，军事人才仅靠在校所学的知识，将不再能够适应未来新军事变革的需要。所以，学校要有针对性的充实教学内容，使学习者随时紧跟信息化发展的步伐。除保证培养学习者学习能力所必需的基础知识的基础上，增加信息化内容。将相关的课程可以合并成一些综合的科目；将已经不适合的内容要删减掉，不能为了怕影响教学计划而保留不合时宜的内容。这样做，一方面有利于学习者自主学习相关的信息化作战和技术理论，同时还可发展他们的兴趣爱好和创造能力留下空间；另一方面有利于给开设一些适应未来信息化条件下的军事理论课程留下时间。还可以激发学习者对学习信息化知识的兴趣，引导他们在学的过程中，发现问题、提出问题、研究问题，系统地学习科学的研究方法，从中培养

信息化综合素质。

(2) 着眼当前部队建设的实际，有针对性地突出专业教学特色

培养信息化军事人才，必须立足当前部队建设的实际，调整专业学科建设，突出教学特色，建设具有信息化特点的学科，推动信息化军事人才培养的发展。

1) 把握不同专业、不同层次信息化军事人才的特点，研究他们的知识、能力和综合素质结构，按照科学系统的授课理念，解决好教学内容和授课体系之间的整体优化问题。

2) 突出专业教学特色，并不是单纯孤立的发展学科教学，要敢于打破各课程间的壁垒，对课程体系进行优化重组，增加反映信息化学科专业交叉融合的综合课程，实现信息化教育、传统基础教育、军事理论教育有机结合。

3) 优化课程体系，更新教学内容。当前在信息化课程的设置中还存在很多问题，改革传统课程体系设计，使其层次上深化、体系上完备。建立系统、开放、灵活、进出有序、机制完善的特色学科，提升特色课程体系的核心地位，以适应信息化军事人才培养的要求。同时，特色学科要适应信息化的进步而不断充实，要适应信息化作战理论的发展而创新，要适应培训对象的不同而不断变化。

(3) 适应现代化教学的需要，有针对性地提升教学保障层次

科学、合理、高效的教学保障是培养信息化高素质军事人才的基础，也是培养信息化人才学科建设的重要组成。提升教学保障层次，应从以下几方面入手。

1) 教学保障应以信息技术为纽带，以实现信息化为目标，整合教学资源，发挥院校技术、人才优势。利用网络将分散的各种资源如：图书馆、教

研究室、实验室、专业教室等整合在一起,着眼学科发展的前沿和专业特点进行保障,为培养信息化军事人才提供信息化环境。

2) 建立新型实验室,贴近信息化战争要求,符合未来战场需要,为培养军事人才提供信息化平台。信息化战争对当前的院校教育提出了新的要求,计算机技术、网络技术、虚拟实验室等现代技术的发展将未来战场搬到了教室以及作战指挥室。加强此方面的保障可以有效增强军事人才对未来信息化战争的预见性,提高作战水平。

3) 合理利用信息技术改造传统学科实验室和网上作战系统,提高原有教学资源的信息化水平和实验功能,为传统优势学科的持续发展创造条件。

## 2 注重提高信息化条件下的实际能力,强化军事人才信息化的专业素质

在于增强其信息化条件下的实际作战能力。而先进的网络模拟训练,则是提高实际信息化作战能力的重要手段。因此,要充分发挥现有信息化设备的效用,采取集训、轮训、代训等各种集约化培训方式,扩大信息化军事人才培养的辐射面。

### (1) 大力发展网络教育

网络教育是依托计算机网络,以多媒体技术、超媒体技术和网络技术等多种手段综合运用的现代化教学手段。网络教育已成为现代教育训练的主要手段。近些年来,我军院校以及部队对网络教育手段非常重视,随着全军教育训练网的开通和各院校对网络资源的开发与共享,网络已经成为培养军事人才的重要手段之一。借助于先进的网络技术,有限的资源得到了充分的利用,达到了信息共享、资源节省、效益提高的目的。充分显示了网络教育模式对我军未来军事人才培养将起到重要的意义,网络教育具有无可比拟的优越性和广阔的发展前景。

1) 利用网络教育,我们可以打破地域和时间的限制,保证对军事人才培养的连续性和实时性。过去,由于距离和时间等不利因素的限制,对军事人才掌握知识的更新和提高是一件十分困难的工作。由于人员的分散性和任务的不确定性,将军事人才进行集中返回院校学习经常达不到预期目的。利用现代化教学手段,依托网络和院校的教学资源,学习者无需在院校集中学习,完全可以由自己制订学习计划,合理安排学习时间。这样,既避免

了对工作的极大影响,又可以保证较好的学习效果,起到事半功倍的作用。

2) 网络教育的交互式教学方法,可以改革传统教育模式。利用军事信息网进行远距离教学,可以充分利用全军院校的师资力量和网络资源。授课教员既可在本校进行网络授课,也可以制作多媒体课件利用网络进行资源共享,这样既保留了传统教学的优点,又可以改变教员教,学员学的填鸭式教学方法。如果在学习过程中,对某一个问题没有理解透彻,学习者既可以对网络教学内容进行反复观看,又可以利用网络留言板和聊天室向授课教员提出问题等待答复。

3) 网络资源的快捷性和全新的阅读方式极大地提高了军事人才自我学习的热情和兴趣。电子书刊和超文本资料库的出现,给学习者带来了观念上的改变,对知识的学习不再是单一的文字和图画样式,超文本阅读将知识从文字扩展为声音、图像、影视等多媒体手段。这种阅读方式将人们从繁重的检索工作中解脱出来,极大地提高了学习的兴趣和效率,而且更易于接受和记忆。

### (2) 科学构建虚拟课堂

虚拟课堂是指通过特殊的输入设备和输出设备,以三维图形和立体音效来模拟人和环境之间虚拟现实的交互系统。虚拟课堂基于多媒体技术,可以模拟建立与真实环境相近的学习场景,是军事人才在学习的过程中感觉置身于逼真的课堂。虚拟课堂所应用的软件除能创造出逼真的课堂教学效果之外,还应具有开放的交流环境,甚至还应具有协助学习者完成学习任务和作业的基本功能。运用虚拟课程实施教育,是 21 世纪军事信息化人才教育训练的一种主要手段。虚拟课堂应具有以下特点。

1) 具有灵活的学习方式。传统的学习方式是按纲施训,而虚拟课堂则是按需而学,学习者可以根据自己的水平选择内容,因人施教。虚拟课堂依托计算机技术和现代网络技术使学习者完全自己把握学习内容和学习时间,有力地解决对信息化军事人才教育中的工学矛盾。

2) 具有完备的学习内容。虚拟课堂使各种基础课程、专业技术课程、应用性知识实现网上共享。学习者根据自己的实际情况或需要学习的相关内容,在虚拟课堂中进行选择性学习,而无需系统掌握内容。

3) 具有丰富的信息资源。利用虚拟课堂中的

学习资源库,学习者可以在虚拟图书馆中方便快捷的查阅各种信息资源,为学习提供参考和依据。通过调阅图文并茂的学习软件,可以有效地改善学习环境,提高培训层次。

4) 具有友好的人机环境。虚拟课堂的软件开发者,应重视对知识结构的理解和充分发挥计算机交互学习的特点。对于具备一定计算机应用技能的学习者,操作界面以及使用方法应能被方便的掌握和使用。学习者可以通过自由选择软件,达到更新知识、开发智力、提高能力的目的。同时,利用虚拟课堂信息中心的信息链应该可以方便地实现与其他教育站点的链接,达到取长补短的目的。

#### (3) 不断更新教育训练手段

近年来,我军信息化建设特别是军事信息网络建设,无论是在基础建设上,还是技术应用上都有了长足的进步,取得了明显的成绩。但是随着信息技术的飞速发展,对军事信息化建设的深度和广度都提出了更高的要求,因此不断更新教育训练手段,培养合格的信息化军事人才,是当前乃至今后一个时期军队人才建设的一项战略性任务。要紧跟信息化发展更新教育训练手段应把握以下三个方面。

1) 强化基础教育。信息化军事人才是军队未来发展的主要力量,强化对军事人才的基础教育是对信息化军事人才培养其他各类要素的发展速度和质量有着决定性影响的关键环节。通过强化基础教育,可以使高素质信息化军事人才具有科学的头脑、扎实的信息基础和高超的信息技术专长。

2) 注重超前教育。军事人才的培养机构应从信息化战争的需求出发,立足当前、放眼未来,对军事信息化技术的前沿学科以及信息化作战理论进行研究,同时坚持不懈地向军事人才普及信息化知识,增强信息化作战意识,培养出大量适应未来军队信息化作战需要的复合型军事人才。

3) 实行开放教育。培养信息化军事人才应将信息资源的合理配置和高效利用作为重要途径,除利用我军现有的信息化资源之外,还应依托国民高等教育,注意当前国际国内信息化领域的发展方向,全方位、多角度、系统化的培养军事人才。对于思想僵化、墨守成规的军事人才要引导他们走出去、向外看、多学习,提高其信息化素质,使其积极地参与信息化建设,最大限度地发挥信息化的效益。

军队信息化对人才的需求是空前的,不断更新教育训练手段,拓宽人才培养的方法,造就一支高素质信息化军事人才队伍是确保我军持续、高效、健康发展的必要环节。

### 3 统筹当前信息化军事人才培养目标,构建信息化较强的教学内容体系

任职教育是按军官的任职岗位逐级实施的,必须遵循信息化军事人才的成长规律,系统筹划培养目标,合理区分教学内容,构建信息化很强的教学内容体系,在教学内容上贴近部队信息化发展,在教学方法上适应部队信息化建设需要。

#### (1) 优化教育机构,体现专业教学的延续性

专业教学的延续性,关键在于打造可持续发展的人才链,建设训战一致的实验平台,而教育机构的优劣决定着培养人才质量的好坏,因此必须首先提高教育人员的综合素质。用超前的眼光不断更新他们的知识结构,打造可持续发展的人才链。而体现专业教学信息化内容的延续性必须紧贴部队实际、紧贴作战任务、紧贴岗位任职需要,加强院校与部队间的代职交流。时军事人才掌握的信息化作战及技术理论同部队的实际相结合。另外,还应适应未来信息化战场的要求,建立训战一致的实验平台和综合实践教学基地,为教学的延续发展提供有力保障。

#### (2) 制定阶段目标,保证信息化军事人才培养的系统性

要保证信息化军事人才培养的系统性,应遵循以下几点。

1) 立足信息化战争需要和信息人才培养目标合理设置专业。根据信息化人才与技能需求,结合军队信息化要求,信息化人才主要包括信息技术研究和开发人才、信息化管理人才、信息技术应用开发人才和信息作战指挥人才四大类。每一类又覆盖若干个军事职业岗位,只有深入研究军队信息化需求与这些岗位的人才要求,才能系统培训出大量合格的信息化军事人才,这是基础也是关键。

2) 基于院校自身条件,合理优化配置资源。军事人才培养的系统性和连续性依赖于必须的教育资源。各院校在培养军事人才时,应根据自身的办学条件和特色,力求使资源合理优化配置,避免教育资源闲置浪费,实现信息化军事人才的系统培养

目标。

3) 要考虑军事人才自身条件, 提供系统课程教育。由于未来信息化战争的复杂性, 信息专业设置不宜过细、过窄。在培养军事人才时要面向未来, 超前培养。拓宽专业设置, 按期使军事人才在不同岗位得到锻炼, 强化他们的专业技能, 培养他们可持续发展的能力和素质, 让信息化军事人才在接受系统培训后能够适应更多的岗位和专业。

(3) 强化专业技能, 注重信息化教材体系的整体性

信息化军事人才培养, 除要重视军事素质、管理素质、信息素质、文化素质和心理素质的培养, 还要重视专业技能培训教学。以信息化教材的编写为突破口, 注重教材的系统性和完整性。教材的编

写, 应依据拓宽专业知识、打牢专业基础的要求编写, 目的是要使军事人才的知识、能力和素质结构更臻完善、科学、合理。

信息技术的发展, 使各种知识爆炸般的增长, 院校教材如果不适时更新和完善就会使学习者的知识结构迅速过失失效。在优化教学内容时, 要以体现当代科学技术加速发展、多学科知识交叉渗透的特征和军队信息化建设的最新成果为重点, 重新审视教材内容, 建立起综合化、现代化、模块化的内容。那种仅靠增加内容和膨胀课时的做法只能使学习者负担过重, 不利于其他素质的发展, 所以对于那些过时、陈旧的内容要坚决摒弃, 形成对信息技术应用学习、追踪和更新的良性循环。

### 参考文献

- [1] 江泽民.《论国防和军队建设》. 北京: 解放军出版社, 2003
- [2] 侯喜贵.《信息化建设研究》. 北京: 解放军出版社, 2002
- [3] 《信息管理论》. 北京: 长征出版社, 2003

### 作者联系方式

通信地址: 陆军航空兵学院管理基础教研室  
邮政编码: 710068  
联系电话: 010-66877702

# 中级指挥院校信息化人才培养之浅见

张立新 马远鹏

**摘 要：**人才是强军之本，兴军之基，培养大批信息化军事人才是军队信息化建设的客观要求，也是中级指挥院校任职教育面临的一项紧迫的现实任务。本文从更新人才培养的观念、科学确定人才培养的目标、拓宽人才培养的渠道、创新人才培养的教学内容体系、优化人才培养的教学方法体系、完善人才培养的机制6个方面，对中级指挥院校信息化人才培养问题进行了初步探讨。

**关键词：**院校教育；人才培养

## 1 更新人才培养的观念

观念是行动的先导，中级指挥院校要培养现代战争所需要的大批信息化军事人才，就必须首先准确把握任职教育的特点规律，树立人才培养的新观念。

### 1.1 人才培养必须突出岗位任职能力

任职教育，最基本的要求是培养受教育者以指挥作战、组织训练、管理部队和思想政治工作为核心的岗位任职能力，强调的是人才培养的岗位适应性。因此，中级指挥院校任职教育必须打破学科专业界限，紧贴各级各类人才的岗位需要，按照培训对象岗位任职所需能力设置课程内容，实施教学。

### 1.2 人才培养必须紧贴作战任务

紧贴作战任务，培养信息化军事指挥人才，是中级指挥院校的第一要务。为此，中级指挥院校必须以培养适应现实军事斗争准备需要的信息化军事人才为目标，紧紧围绕各级各类人才在未来作战中可能担负的作战任务，突出部队信息化建设急需人才和急需知识，加强新理论、新战法、新技术、新装备的教学，加强使命课题的训练，不断增强人才培养的针对性。

### 1.3 人才培养必须强化实践教学环节

与学历教育相比，中级指挥任职教育更加重视传授经验、注重应用、培养能力和突出实践环节。中级指挥任职教育，在人才培养过程中必须针对该培训特点，充分利用基地化、模拟化、网络化、综

合演练的训练环境和条件，加大实践性教学环节的的力度，增加实装操作、实地指挥、实地作业训练的比重，加强实际岗位锻炼，促进受教育者理论、知识向能力、素质的转化。

## 2 科学确定人才培养的目标

中级指挥任职教育人才培养，应以毛泽东军事思想、邓小平新时期军队建设思想、江泽民国防和军队建设思想为指导，以新时期军事战略方针为统揽，以军事斗争准备为牵引，以推进军队由机械化条件下军事训练向信息化条件下军事训练转变为主题，深入贯彻落实科学发展观，采取超常措施，培养政治立场坚定，具有信息化的军事思维观念，知识、能力、素质兼备并具有较强创新能力、适应信息化战争需要的复合型军事人才。

### 2.1 具有较强的政治敏锐性和政治鉴别力

要通过马克思列宁主义、毛泽东思想、邓小平理论、“三个代表”重要思想和科学发展观的学习，增强政治敏锐性和政治鉴别力，树立坚定的政治立场和正确的政治信仰，坚守政治纪律，坚持党对军队的绝对领导，在思想上、政治上、行动上自觉同党中央、中央军委保持高度一致。

### 2.2 具备信息化的军事思维方式

信息时代，信息已经从战斗力的一种辅助因素，上升为同火力、机动、指挥和保障并列的战斗力要素，并且信息在集成战斗力要素上具有纽带作用。因此，信息化军事人才，应适应战争形态由机



械化战争向信息化战争转变的客观要求,变机械化军事思维方式为信息化军事思维方式、变单项思维为多项思维、变封闭思维为开放思维、变保守思维为创新思维。中级指挥任职教育应将受教育者信息知识掌握的多少、信息运用的程度作为检验教学水平的首要标准,按照信息化要求制定人才培养方案,改革人才培养模式,提高人才培养质量。

### 2.3 知识、能力、素质兼备,“指技合一”,具有较强的创新能力,富有战斗精神

从人才构成的要素看,知识、能力、素质作为人才结构体系的三大要素,密不可分。其中,素质是知识、能力赖以存在和发展的基础,优良的素质有利于知识和能力水平的发挥和提高;而知识和能力是素质的主要条件和外在表现,知识的获得有助于能力的提高,知识的获得和能力的提高又能够促进素质结构的完善和更新。因此,中级指挥任职教育,不仅要强调知识传授和能力培养,而且更要注重全面提高受教育者的综合素质。

由于现代战争要求指挥人员不仅要懂指挥、会管理,而且要懂技术、会运用,所以在任职教育实施过程中,不仅要给学员讲授战役战术、作战指挥、部队管理理论,还要给学员传授高技术武器装备的战术使用、维护保养、技术保障等装备技术知识,做到指挥与技术有机结合,以培养复合型的军事指挥人才。

江泽民同志在 1995 年全国科学技术大会上曾经指出:“创新是一个民族进步的灵魂,一个没有创新能力的民族难以屹立于世界先进民族之林。”新的世纪是创新的世纪,国与国之间的竞争、战争的竞争,在很大程度上是创新能力的竞争。所以军事指挥人员不仅要知识、能力、素质兼备,而且还要具有较强的创新能力,这是适应信息时代要求的必然选择。其一,应具备信息化条件下的技术运用和创新能力。其二,应具备信息化军事理论创新能力。

战斗精神,是军队信念、信心、勇气、意志和高昂士气等精神状态的集中反映。物质手段的改进,推动着精神世界的发展。不同形态的战争,对战斗精神提出了不同的要求。冷兵器时代的战争,战场范围较小,作战双方刀兵相接,需要的是以“勇猛无畏、敢打敢拼”为核心的战斗精神。热兵器时代的战争,战场范围扩大,并且出现了海洋战

场,需要的是以“坚定沉着、机智勇敢”为核心的战斗精神。机械化战争,战场范围由陆地、海洋向空中扩展,交战规模空前扩大,历时旷日持久,在以“消灭敌有生力量”为主要目标的作战思想指导下,破坏与残杀的程度愈演愈烈,需要的是以“连续作战、英勇顽强”为核心的战斗精神。信息化条件下的局部战争,战场空间向陆、海、空、天、电、信(认知领域)融为一体的方向发展,平台中心战被网络中心战所取代,信息化战场环境中,需要的是以“精密协作、处变不惊、多谋善断”为核心的战斗精神。所以,信息时代的战斗精神,是各个战争时代战斗精神的继承与发展,在战争中的地位更加突出。也就是说,现代战争对参战人员的精神因素提出了新的更高的要求。因此,军事指挥人才必须具备坚定的政治信念、顽强的战斗意志、过硬的战斗作风,牢固树立敢打必胜的坚定信心。

## 3 拓宽人才培养的渠道

### 3.1 充分发挥军队院校军事人才培养的“主渠道”作用

培养大批信息化军事人才,必须把院校教育摆在优先发展的战略地位,充分发挥军队院校培养军事人才的“主渠道”作用。在充分认识院校教育“基础性、全局性、先导性”地位的同时,应从培养新型军事人才的需要出发,深化院校教学科研改革,实现人才培养的“两个转变”:其一,由单一结构型向复合结构型转变。部队建设的合成化和训练、作战的一体化,要求军事指挥人员掌握新知识、新装备、新技术、新战法和新理论,实现军事指挥、政治工作、后勤和装备保障的复合,指挥、管理和技术的复合,学术科研和军事应用的复合。其二,由应试教育向素质教育的转变。从注重知识的传授和灌输转向注重能力的培养和素质的提高,不断提高人才的适应能力、创新能力和后续发展能力。

### 3.2 依托国民教育培养军事人才

依托国民教育培养军事人才,是世界各国军事人才培养的一个趋势,也是我军人才培养的重大改革。部队作战所需的通用性专业人才可以从地方招募补充,指挥军官的学历教育和部分专业的继续教

育也可以在地方院校完成。为此,军队院校要撤消内容设置与地方院校相同或相近的学科,将部分培训对象和内容移交给地方院校,充分利用地方院校教学设备先进、师资力量雄厚的优势,为军队培养更多的专业技术人才;改革军事教育体制,建立与国民教育接轨的军地联合办学体制;进一步加大军校开放办学的力度,加强与地方院校的交流与合作。

### 3.3 建立院校、部队和科研机构共育人才机制

院校、部队和科研机构在理论教学、实践锻炼、学术科研等环节上分别扮演着不同的角色,都具有不可替代的作用。充分发挥院校、部队和科研机构在人才培养上的综合优势,探索联合培养模式,建立共育人才机制,形成整体合力,是培养信息化军事人才的客观要求。院校应通过有计划地组织教员到部队调研、实习和代职锻炼,主动了解部队作战训练对人才素质的要求,学员岗位任职所必须的知识、能力和素质,特别是要了解新装备的发展趋势,为部队训法和战法改革、为院校教学科研提供人才与技术支持。部队应通过选派实践经验丰富、素质高、能力强的优秀军官到院校介绍部队情况或任教,充实教员队伍,改善教员队伍结构,将部队岗位任职需要、对院校教育的意见及时反馈给院校。

### 3.4 加强岗位锻炼和在职培训

组织不同专业、不同层次的人员进行集中培训,使人才的知识、技能不断更新和补充;打破不同军兵种和不同专业的界限,抓好同类干部、不同兵种干部的岗位互换,抓好军政、指技干部之间的交叉换岗,抓好机关与基层干部之间的双向交流,全面提高干部的综合素质。

## 4 创新人才培养的教学内容体系

教学内容关系到培养人才的知识、能力和素质结构,所以,教学内容改革始终是教学改革的核心。目前,我军现行的课程体系大多是在传统的应试教育思想指导下建立的,或多或少地残留着应试教育的烙印,与任职教育的要求不相适应,突出表

现在两个方面:一是课程内容陈旧落后,高、新技术知识含量较少,不能满足现代战争的需要;二是课程内容设置上存在着重知识传授、轻能力培养和重必修课、轻选修课的现象,导致学员理论知识陈旧、知识面狭窄、创新思维能力缺乏、素质偏低,不能满足部队建设和未来作战需要。为此,在构建中级指挥任职教育课程体系时应突出“四性”。

### 4.1 岗位性

学历教育注重受教育者的长远发展,侧重全面打牢基础;任职教育具有鲜明的岗位指向性,注重岗位任职的现实需求,侧重培养受教育者的岗位任职能力,强调人才岗位的适应性。因此,在构建中级任职教育课程体系时,应紧紧围绕军事斗争准备、部队建设实际、不同的职业岗位要求,以培养学员岗位任职能力为重点,以适应任职岗位为准则,为学员岗位任职需要打下坚实的基础。适应岗位任职需求,是构建中级指挥任职教育课程体系的基本依据。

### 4.2 实践性

在构建中级指挥任职教育课程体系时,在保证基础理论教学要求的基础上,加大应用理论教学的比重,注重实践能力的培养,提高解决实际问题的能力。

### 4.3 前瞻性

在构建中级指挥任职教育课程体系时,既要满足学员第一任职需要,又要照顾其未来发展,既要让学员有较好的岗位适应能力,又要有较好的发展潜力。为此,在教学过程中,既要注重基础理论、基础知识和基本技能的讲授,又要注重新理论、新知识、新技术、新战法的学习,不断更新教学内容,使教学内容具有较强的前瞻性。

### 4.4 复合性

信息化战争,要求指挥人员具有良好的职业道德意识、过硬的军事素质、较强的组织管理能力和丰富的科学文化知识。为此,在构建中级指挥任职教育课程体系时,要着眼军队信息化建设要求,搞好人才培养的顶层设计,突出学员四种能力的培养:掌握专业知识和技能,具有较强的作战指挥能

力；掌握军事训练理论和知识，具有较好的教学素养和组训能力；掌握基层管理方法，具有与任职岗位相适应的领导管理能力；掌握经常性思想政治工作的原则方法，具有做思想政治工作特别是战时思想政治工作的能力。满足培养具有指挥作战、组织训练、管理教育和基层政治工作能力的复合型军事人才的需要。

此外，教学内容应注重培育战斗精神、提高打赢能力。著名军事理论家克劳塞维茨指出，战斗力“是两个不可分割的因数的乘积，这两个因数就是现有手段的多少和意志力的强弱。”“军人的勇气和士气在过去各个时期都曾使军队的物质力量成倍地增强，今后仍会这样。”打赢战争，最根本的就是对敌方意志的征服。为此，要从紧贴形势任务强化思想教育方面入手，着力培育官兵坚定的政治信念、顽强的战斗意志、过硬的战斗作风；要通过开展“人与武器装备的辩证关系”、“决定战争胜负的因素是什么”等讨论，引导官兵充分认清无论武器装备如何发展，决定战争胜负的根本因素依然是人，只要苦练精兵，充分发挥人的主观能动性，熟练掌握手中武器，就一定能在未来战争中掌握主动权；通过介绍新装备、讲解我军光荣传统和成功战例、讲清新世纪新阶段我军肩负的历史使命等，引导官兵更加清醒地判断形势，更加清醒地认识职责使命。总之，要通过深入进行强化战斗精神、提高打赢能力教育，真正搞清楚为什么要准备打仗、准备打什么样的仗、怎么准备打仗这个重大问题，引导广大官兵牢固树立敢打必胜的坚定信心。

## 5 优化人才培养的教学方法体系

教学方法是教员和学员在教学过程中，为了达到教学目的，完成教学任务，在教学活动中采取的手段和方式。教学方法是实现教学目的、落实人才培养目标、提高教学质量的重要因素。因此，要培养学员的创造能力和创新意识，必须深化教学方法改革。

### 5.1 针对不同的教学对象和教学内容因人、因材施教，加强针对性教学

在教学实施过程中，应针对不同教学对象的特点，在总的教学大纲指导下，制定具体的教学实施计划，在教学内容设置上区别对待，各有侧重。首先，要针对不同的教学对象因人施教。其次，要根

据不同的教学内容因材施教。

### 5.2 重视“学法”研究，突出学员的主体地位，变“以教为主”的教学旧模式为“以学为主”的教学新模式

教学方法由教的方法和学的方法两部分构成，是二者的统一体。教法与学法如车之两轮，两轮同时转动，教学之车才能正常运行。在教学过程中，教员的主导作用只是外因，而学员的主动性才是内因，外因只有通过内因才起作用。古人云：“授之以鱼，不如授之以渔”。因此，在改革教学方法时，必须贯彻“教为主导、学为主体”的指导原则，注重学法研究，充分发挥学员的主体作用，进一步加强学员自主、自控能力的培养，把主要精力放在对学员学习能力的提高上。

### 5.3 突出实践性教学环节，注重学员能力与素质的培养

首先，要强化实践教学观念。在教学内容的设计上，不仅要注重基础理论知识的讲授，更要注重实践能力的培养，做到理论教学既要为实践教学服务，又要指导实践教学的开展。其次，要积极实施启发式、研讨式、问题式、案例式教学，加强教学互动，变教学方法上的“注入式”为“启发式”、变“单向输入”为“双向交流”，培养学员创新思维、创新意识和创新精神，提高其获取新知识、新理论的能力，并针对不同的教学对象，将多种方法有机结合起来，以提高教学效果。要注重教学方法的整体性，把教授与自学、研讨与交流等灵活多样的教学形式结合起来，通过科学的教学设计、严谨而灵活的施教方式，激发学员学习兴趣。要鼓励学员应用直觉思维和求同存异、灵活变通，能从不同角度思考问题，把握宏观思路，讲透方法重点，为学员留出思考、创新的空间。

### 5.4 改革考试方法，建立科学合理的评价机制

考试是检验教学、促进教学活动的一种手段，是教学活动的“指挥棒”，是任何教育模式都不可忽视的。教学实践经验表明：学员往往是根据“考什么”和“怎么考”，支配自己“学什么”和“怎么学”，进而对教员提出“教什么”和“怎么教”的要求。换言之，学法是教法的前提，而考法是学

法和教法的指南。为了适应中级指挥院校任职教育需要,培养新型军事人才,必须改革过去“应试教育”的考试方法,变单纯检查知识水平的考试为综合素质考试,变重点考查学员的知识和记忆能力为重点考查学员的实际操作能力、理解运用能力、创新思维能力,通过对学员的全面素质进行科学综合的检验,得出正确的评价结论。在中级指挥任职教育考试过程中,应坚持知识、能力、素质三位一体和军事、政治、科技有机融合,打破课程界限,由单科考核向综合性考核、联合答辩式考核转变。针对专业特点,可采取笔试与口试相结合、撰写论文与综合考试相结合、理论考试与技能考核相结合、课堂提问与课终考试相结合等多种方式,以促进学员综合素质和能力的培养。

## 6 完善人才培养的机制

人才培养机制完善与否,直接影响到人才培养的质量。为此,中级指挥院校信息化人才培养,必须完善人才培养的机制,创造有利于人才脱颖而出的良好环境。

### 6.1 建立高效权威的领导管理机构

由于中级指挥任职教育具有培训对象多元化的特点,无形之中增大了教育管理的难度,对教育管理提出了更高的要求。为此,应充分发挥院校与部队合力育人的优势,建立由总部机关牵头、院校为主与部队相协调的三位一体的组织管理机构与运行机制。总部机关负责制定任职教育中一些重大的政策法规与实施办法;院校要切实履行教育管理的主体作用和集体干部部的作用,注重对受教育者在校学习期间的综合考察,并将受教育者在院校的表现情况及时反馈到其部队单位领导;部队要将个人在院校的学习、工作表现与其职务晋升相联系,以达到齐抓共管、合力育人之目的。

### 6.2 完善与实施全程管理机制

中级指挥任职教育的实施过程,主要包括选送、培训、考核、使用四个关键环节,任职教育实

施过程中,要针对这四个环节建立相应的规章制度,对培训对象实施全程管理。其一,部队要严格按照学员选送标准和培训目标要求择优选送学员;院校要严把招生关,保证生源质量。其二,培训过程中要认真落实教学计划,严格执行考核制度,实施全程淘汰机制。其三,严格落实不训不晋、预晋先训、训用一致制度,对成绩突出的优秀学员做到优先使用、优先晋升,充分发挥政策的导向作用,激励学员学习的积极性、主动性,这是任职教育得以健康快速发展的关键所在。

### 6.3 优化人才成长环境

部队各级领导要把培养、吸收和用好人才作为一项重要的战略任务抓紧抓好,努力营造吸引人才和尊重人才的浓厚氛围,创造有利于人才脱颖而出的良好环境。首先,要用正确的导向凝聚人才。对那些既懂军事又懂政治、既懂指挥又懂技术和管理各类人才,看准了要大胆使用,对在部队信息化建设过程中涌现出来的先进典型,发现了要大力宣扬,努力形成尊重劳动、尊重知识、尊重人才、尊重创造的良好氛围,各级领导干部要率先垂范,带头学习、运用高科技知识,自觉当好部队信息化建设的排头兵,以实际行动影响和带动部队官兵,为实现军队信息化建设的跨越式发展做出应有的贡献。其次,要用有效的机制激励人才。要在继续完善落实干部目标责任制的同时,积极推行和实施干部任职公示制度、任前考核制度,形成一整套有利于人才培养和使用的激励竞争机制。要坚持任人唯贤,反对任人唯亲;既要德才兼备,又不求全责备;既要坚持标准,又要不拘一格。形成人尽其才、才尽其用的良好局面。第三,要加强人才战略工程的法规制度建设。部队各级党委要加强对人才建设的集中统一领导,在加强院校教育、在职学习、岗位锻炼的同时,加强青年干部培养工作的力度,做好干部交流任职工作,完善吸引保留人才的激励竞争机制,加大人才培养投入力度,建立健全与实施人才战略工程相适应的法规制度,确保中央军委确定的人才战略工程规划如期实现。

参考文献(略)

作者联系方式

通信地址:河北宣化炮兵指挥学院装备技术教研室 邮政编码:075100 联系电话:0313-3366338 13283305228

# 浅议侦察情报战线信息化人才培养与一体化训练

赵磊

**摘要:**所谓信息化,就是在军队作战体系及其日常运行中,深度掌握和普遍运用先进的信息技术,建成一大批信息化装备系统和传输网络,极大提高信息的获取、存储、处理、传输、利用以及安全防护等能力,有效增强指挥决策、侦察监视、战略预警、通信传输、火力打击、力量投送、物资保障和战备训练等方面的运行效率与综合效能。所谓一体化训练,是指为熟悉联合作战体系及其运作,密切协同配合,提升联合作战能力,以一体化信息系统为依托,将分散配置的各作战要素、作战单元连成一体,而进行的高度集成的训练。

新军事变革中的我军信息化建设,是强军之路,是战力之本,是“打赢”之基,从本质上看,其进程与成败取决于信息化人才队伍的素质与能力。贯彻落实全军信息化作战体系建设的总体部署,加速构建和用好用活全维一体的侦察情报体系,适应一体化联合作战要求,必须面向侦察情报工作信息化建设的进程,面向未来联合作战的组织保障模式,坚持一体化训练,积极打造理念新、视野宽、懂作战、善协作的侦察情报人才方阵。本文从侦察情报战线信息化建设的重点任务和特点规律入手,分析了人才素质要求,对搞好一体化训练提出了对策建议。

**关键词:** 侦察; 一体化训练; 人才培养

## 1 准确把握侦察情报工作信息化建设的特点规律

侦察情报工作信息化建设,就是在加快完成机械化补课任务的同时,大力推进信息化进程,在侦察情报战线的各个领域、各个环节、各个方面,广泛运用信息技术,全面加强侦察情报体系网络化、侦察手段广谱化、功能要素集成化、信息处理智能化等建设,重点推动信息基础设施建设、装备信息化建设、作业流程模式与管理保障机制信息化建设、支撑环境信息化建设以及信息化人才队伍建设,形成多维一体的广谱侦察监视能力、多源信息融合处理能力、一体化指挥控制能力、高效安全信息传输能力,以及攻防兼备的信息对抗能力,充分开发各种情报信息资源,从而全面提高情报保障能力的全部活动,它是军队信息化建设的重要组成部分,并具有以下特点。

### 1.1 装备富含高新技术,科研攻坚难度空前

侦察情报工作是以知识技术为依托在信息领域与敌较量,不断获取决策指挥与部队行动所需情报的艰巨性、对抗性工作,是夺取信息优势和作战主

动的重要前提。这项工作涵盖通信信号侦察、电子侦察、图像侦察、网络侦察、核爆探测、战场侦察监视、测量与特征目标识别等手段和领域,集成了多门类高新技术学科,并有力牵引信息技术研发和最先运用其高端成果。随着世界信息技术的迅猛发展,新理论、新技术、新材料、新产品层出不穷,科研成果转化为产品的周期大大缩短,给侦察情报工作带来了前所未有的技术挑战。针对发达国家特别是战时复杂电磁环境下开展侦察,更需要跟上网络时代信息技术的发展前沿,努力在卫星平台、近空平台、海空基平台及其载荷技术,雷达探测、遥感遥测、红外远红外技术,低截获率信息侦获技术,细微特征提取利用技术,信息系统网络安全机制突破技术、海量信息智能筛选、识别、解译技术,目标高精度测向定位技术,量子密码、生物密码以及量子计算、生物计算技术,激光通信技术,信息栅格技术、神经网络技术,多源情报信息融合技术,攻击预警技术等方面,以及纳米、超导、微加工等新材料新工艺上不断取得突破,攻克制约信息化装备研制的关键难题。

### 1.2 侦察资源广域分散,整体联动势在必行

由于侦察情报力量分属于总部与各个军区、军

兵种,多年来,从建立适当侦察覆盖,获取战略战役情报以及当面海空态势为主的战场监视情报需要出发,侦察阵地的建设部署形成了点多、线长、面广、分管的格局,不仅涉及天基侦察、空基侦察、海基侦察、陆地侦察、境外侦察等平台,而且覆盖主动侦察、探测、观测、攻网与被动信号截收处理等侦察手段,牵动多个部门与多个侦察系统。必须从加强丰富信息资源开发利用,加强侦察阵地平台综合利用,以及改善情报相互关联、印证,提高完整性与可靠性出发,以网链接、综合集成,整体联动、共享开发,是必然的发展趋势。

### 1.3 情报信息量大类杂,共享融合迫在眉睫

信息化网络化的迅猛发展,使各种通信、非通信信息资源急剧增长,并发生了结构性变化,特别是网络信息数量大得惊人。通过发展新手段,攻研新技术,研制新装备,侦察情报系统的信息侦控能力将持续大幅度提高,图像数据、雷达探测数据、电磁频谱监测数据以及从各种通信系统网络中截获信息的总量呈指数上升,语音信息、文本信息、数据信息、传真信息、图像信息、视频信息数量剧增,在相当长的一段时间内,对不同侦察对象、不同语种、不同媒介形式的多元化丰富信息资源的处理筛选,将成为突出问题。

### 1.4 装备系统体制迥异,互联兼容标准为先

随着我军侦察情报系统的信息化建设不断推进,多维一体的侦察情报体系将逐步构建,全维、全时、全天候的通信侦察、电子侦察、成像侦察、核爆探测以及战场侦察监视将得以实现,但真正做到建制成体系建设,生成战斗力和保障力,各个阵地、多种手段、不同系统按照任务要求和相关规则实现互联互通互操作,必须在技术体制、接口标准、传输协议和数据格式等方面明确权威部门,建立统一标准,推广统一制式,确保资源统合、力量整合、部门联合及信息融合。

### 1.5 信息安全形势险峻,防护措施亟待加强

信息安全是确保制信息权的重要方面,在信息化战争中,不能确保己方的信息安全,就会丧失战争的主动权。随着我军信息化建设的全面推进,信息资源急剧增长,作战指挥和高技术兵器对信息系

统网络的依赖性越来越强,信息安全已经成为打赢信息化战争、完成祖国统一大业的关键因素。但是,我军信息安全保障工作起步晚、底子薄,总体水平落后,管理漏洞多。一是在用的操作系统、大规模集成电路芯片和高速路由器等高端产品主要依赖进口,关键技术都掌握在他人手中,网络和信息系统暗藏“芯病”,信息安全存在“软肋”,短期内很难摆脱受制于人的被动局面。二是信息安全建设相对滞后,经费投入较国外要少得多,经常是先建网络、后加安全,技术水平也不高,难以形成有效的整体防范能力。三是管理相对落后,信息安全方面的政策、法规和技术标准不健全,对于已有政策规定也存在责任不落实、管理不到位问题,许多网络不经安全检查就开通使用,信息安全管理机构不健全,技术人员缺乏。

近年来,美国、台湾和日本等也都千方百计加大对我的侦察情报活动力度,积极发展情报合作,对我信息安全构成了严重的威胁。可以说,信息安全问题不能妥善解决,将成为制约我军信息化建设的心病和隐忧,甚至羁绊和瓶颈。

## 2 深刻认识信息化建设对侦察情报人才素质的要求

基于上述认识,侦察情报系统必须从当代科学技术发展和世界军事变革的规律上把握潮流大势,贯彻落实科学发展观以人为本的精神,自觉从人才队伍建设这个根本上出思路、谋对策、用实劲,以适应形势和任务。为此,必须首先搞清信息化建设对侦察情报人员的素质要求。

### 2.1 一是必须在观念更新和前沿跟踪上有锐意

侦察情报工作的信息化建设,历来走在军队信息化建设的前列。信息化建设对侦察情报人才素质的要求,首先体现在思想观念、进取精神以及洞察力和敏感性方面。不注意掌握与开展侦察情报工作紧密相关的信息技术发展动向,敌侦察情报技术、理念与模式的最新变化,不善于在信息时代的军事变革中积极研究和深入探索侦察情报工作建设发展的特点规律,就难以对信息化建设主动开拓、多做贡献;就难以在网络化的情报生产流程中适应要

求、积极协作,也就难以在信息安全防护上认识到位、行动自觉。

## 2.2 二是必须在知识渊博和技术精深上有造诣

侦察情报工作是军队高新技术最集中、技术水平最先进的行业和领域。不掌握扎实的通信知识、网络知识、计算机技术和多媒体信息处理技术,以及情报甄别、选取、关联、整编与融合技能,就不可能具备攻关破堡的本领,就缺乏胜任侦察情报工作的基础,也难以跟上随信息技术日新月异而飞速演进的侦察技术发展。

## 2.3 三是必须在协同攻研与联合作业上有素养

网络化时代的侦察情报工作,由技术发展带来的影响广泛而深刻,侦察领域、侦察手段、侦察技术、侦察装备的新进化,不断引发思想观念、体系结构、资源配置、组织模式、运行机制等方面的一系列深刻变革,促使技侦情报工作不断由工业时代的形态向信息时代的形态转变。侦察情报人员必须善于合作、善于借鉴“他山之玉”,汇集和利用好多种知识成果,才能有所作为。

## 2.4 四是必须在参与决策与指挥协调上有能力

侦察情报活动贯穿未来战争整个过程和全方位、各层面,对作战决策指挥与部队行动关系密切,主动到位地做好情报保障与支援,必须懂作战、通指挥、善参与、能协调。必须善于把作战需求转化为情报任务的搜集指南和情报活动的联合行动方案;把情报成果转化为首长的认知决策优势和部队的作战行动优势。

# 3 对搞好一体化训练推进人才培养的初步看法

积极推进一体化训练,是实现我军新形势下作战能力跨越式发展的重大举措,对推进中国特色军事变革,加速我军信息化建设,打赢未来信息化战争,具有重要现实意义和深远战略意义。一体化训

练包括作战单元内部集成训练、作战要素集成训练和作战体系综合集成训练,通过系统集成的方法,实现各种作战力量的有机链接、高度融合,最终生成和强化一体化的联合作战能力。具体到我军侦察情报战线,作为信息技术密集的特殊方面军,一体化训练应当做到5个突出,积极开展三项工作。5个突出是:一体化训练应突出强化信息化知识与信息化理念;应突出强化信息化侦察装备驾驭能力;应突出强化网络化工作环境适应能力;应突出强化协同式攻关的能力与素质;应突出强化参与指挥决策与支援能力。三项重点工作如下。

## 3.1 狠抓集成训练,筑牢一体化训练的根基

### 3.1.1 加强一体化训练理论研究

对我军而言,一体化训练是一个全新的科技练兵概念,是对传统训练思想、手段和方法的革命。要科学指导和正确推行一体化训练,必须创新基础理论,夯实知识根基,以先进、成体系的训练理论作为指南,提高官兵认识,统一思想行动。一是要充分发挥在情报信息获取和对外军研究方面的优势,深入研究世界新军事变革特别是一体化联合作战特点规律和发展趋势,跟踪研究世界发达国家一体化作战理论和建设进展,用辩证、联系、发展的观点,吸收借鉴美军、台军的成功经验,为形成和创新具有中国特色的我军一体化训练理论提供参考。二是要紧密结合侦察情报工作实际,深化对未来作战保障需求和特点规律的研究,从“战、建、训一体”的角度,抓紧一体化侦察情报保障体系的规划设计,为侦察情报系统内部集成建设和训练提供依据。三是要根据全军一体化作战总体要求和一体化建设、训练的整体部署,创新侦察情报训练工作机制,研究形成规范有序的训练制度和科学有效的训练方法,积极探索和提升侦察情报集成训练理论,为训练工作健康发展提供保证。

### 3.1.2 强化基础性集成训练

一是着眼打赢练协同。要围绕打赢目标,按照打赢标准,贯彻一体化联合作战要求,从难从严开展训练。针对侦察情报单位普遍专业工种多、侦察手段杂、阵地分布广的特点,将集成训练渗透到现实战备值勤各个方面、各个环节的协同中,通过与主要作战对手面对面的侦察情报实践活动,不断积累情况、熟悉特点、摸索规律,改进组织管理,完



善协同机制,形成练/打兼用,平时好操作、战时见效益、高度集成的侦/防预案和流程,力求在平时就做到练熟、掌握。**二是针对问题练功力。**要按照战时一体化联合作战情报保障的要求,不断改进薄弱环节和解决存在问题,扎扎实实地打好情报保障的基础。严密跟踪作战对象通信电子技术变化,加快发展侦察技术,针对当前存在的机动侦察能力和前沿阵地抗毁能力弱、系统互联互通性差等问题,依靠科技创新,组织联合攻坚,在解决新问题和疑难问题中练就“应变、攻坚、制胜”的真本领。**三是按照战时情报保障预案练对抗。**要按照仗怎么打就怎么练的原则,大力加强近似实战的情报保障训练。利用每年敌军重大演习,舰机编队在我当面活动以及国际重大突发事件等时机,按照战时要求,开展一体化联合作战情报保障集成训练,全面检验、提高组织指挥、侦察处理、情报融合、情报分发和信息防御能力,不断完善战时情报保障预案,改进和加强情报保障工作。

### 3.1.3 切实抓好侦察系统纵向集成训练

要按照全军一体化联合作战体系的集成要求,重点训练三种主要侦察要素的集成:**一是多种侦察力量集成。**要加强联合侦察组织指挥研究和训练,积极探索在现行指挥体制基础上,依靠信息化、网络化手段,实现多种侦察力量有效合成的途径。**二是多种侦察手段集成。**要加强多手段一体化联合侦察监视训练,围绕对作战对象全面侦察监视能力的提高,探索、演练机动平台与固定侦察平台相结合、主动探测手段与被动接收手段相结合、通信侦察与电子侦察及网络侦察相结合的战术技术方法。**三是多个侦察专业集成。**要加强全军情报力量信息收集、信息处理、情报融合、情报分发等多个工作环节的整体集成训练,统一信息格式、技术标准和数据规范,提高信息传输能力及互联互通水平。要组织全军或区域性侦察情报保障训练,练指挥协同,练侦察机动,练保障防护。通过多种类型的系统内部集成训练,演练多种作战条件下侦察情报工作的战术技术,探索战时情报保障工作的特点和规律,加快侦察力量、侦察手段、情报生产流程高效集成的进程,实现多种侦察情报要素的有效融合,促进保障能力的提高。要切实加强训练的组织指导,优化科目设计,改革训练内容,按实战要求认真总结训练经验教训,不断将一体化训练推向深入。

## 3.2 参与联合训练,提高总体作战效能

提高一体化联合作战能力,不仅要求情报部门有很强的侦察监视、信息处理和情报研究能力,而且要求情报信息与指挥控制、火力打击、综合保障等多种作战要素紧密结合、高度集成,实现从侦察认知向精确打击的高效转化。侦察情报保障工作训练,必须在做好系统内部集成训练的基础上,积极参与全军联合作战体系的联合训练。**一是加强对作战部队的情报保障训练。**要按照统一安排,积极参与全军重大演习训练活动,促进情报部门与部队熟悉了解作战部队的情报需求特点、情报使用规律,作战环境与作战协同,也促进作战部队对情报部队与情报产品的熟悉了解,不断改进情报搜集、处理、分发与应用工作。要按照战时一体化联合作战要求,明确与有关参战单位的通报关系,建立相应的通信传输手段,开展经常性连通试验和模拟演练,实现侦察情报与我军作战指挥控制、打击武器、作战单元与综合保障等作战要素的互联互通、无缝连接。同时,按照条令条例,建立有效协同机制,不断演练侦察力量部署展开、机动前出和及时撤离等行动与火力打击的配合,提高侦察情报力量随行作战部队行动、相互支援和取得保护的能力。**二是加强与有关信息作战部队的协调配合训练。**要提高我军整体信息作战能力,需要以电磁攻击和火力打击等方式干扰、压制和摧毁敌军核心信息系统及网络节点,需要保护我军重要情报来源,也需要确保我军信息系统的安全。为此,要加强与电子对抗部门协同,及时交流电子侦察信息,协调侦察情报与电子攻击的目标、时机,加强协同训练,保证既有效瘫痪敌核心信息系统,又有利于侦察情报工作持续开展。要加强与我军火力打击的协调,共同确定火力打击的目标、顺序,强化协调演练,以保护好重要的情报来源。要加强与我军防御性信息作战力量的协调配合训练,为我军信息安全提供战略预警信息和技术支持。**三是加强各侦察情报部门之间的协调配合训练。**我军侦察卫星、侦察飞机、侦察舰船等大型侦察平台,分属不同部门管理,承载侦察手段类型多,截获情报信息各具特色。要提高一体化情报保障能力,需要加强各有关情报部门的协调配合,制订和演练协同程序,以根据联合作战情报保障的需要,动态调整侦察平台部署,充分发挥所获信息的作用,实现侦察设施共用、侦察成果共享和多种情报信息的融合。



3.3 加快重点平台建设，促进一体化训练成果转化

对全军而言，要以一体化联合作战体系建设为支撑，搭建网络化、一体化作战和训练平台，积极探索“战、建、训”一体的部队建设新模式，加速理论研究成果向作战能力的转化。应根据军委的战略部署，以尽快提高应急作战能力为目标，抓住影响一体化联合作战能力的薄弱环节和突出问题，着眼提高陆、海、空、天、电多维空间作战能力，增强侦察预警、指挥控制、机动、打击、防护和保障各作战环节整体协同能力，在深入研究论证的基础上，确定全军统一建设的重点，集中军内外科技力量，加大投入，突出抓好战场态势综合信息系统、移动目标情报融合系统、侦察—打击—效果评估一体化系统、信息网络攻防一体化系统等一体化情报保障和训练平台建设，抓紧建成一批将作战理论研究、作战平台建设与战术训练活动融为一体、贴近实战环境的网络化平台、联合作战研究实验室和训练基地。侦察情报力量，要改变多年来在作战演习

参考文献（略）

作者联系方式

通信地址：北京市 984 信箱 100 号  
邮政编码：100091  
联系电话：010-66778168

训练中缺位或陪衬的状况，在加强专业训练的同时，研究开发贴近实战环境的网络化平台和训练手段，寓训于战，以战带训，以训促战，战训一致，加快训练成果向战斗力的转化。当前与今后一段时间，要集成一体化联合作战情报保障、信息攻防理论研究一体化体系建设的成果，积极创造条件，采取理论研讨、网上作业、实兵演习等多种方式，会同有关部门抓好战区三军联合情报保障训练、侦察情报与指挥控制联合训练、侦察情报与打击兵器一体化联合训练、军事设施与大型武器系统的反侦察联合训练、网络安全与防御等联合作战科目训练。

4 结束语

一体化训练是各全新的课题，在思想认识、理论研究、保障条件、组织管理等诸多方面还缺乏软硬件基础和实践经验，需要大家共同探索。文中观点粗浅偏颇难免，敬请指正。

# 复杂电磁环境下电子对抗部队一体化训练面临的困难与对策

周永生 王峰辉 黄海松

**摘 要：**复杂电磁环境是信息化战场环境的重要组成部分，一体化联合作战是我军未来主要的作战样式。积极推进复杂电磁环境下的一体化训练，是满足未来作战需求、增强训练实战化程度的重要环节，是电子对抗部队必须应对的现实而紧迫的任务。但作为一种全新的训练实践方式，在训练内容的确定、训练环境的认知与构建、训练方法的选择、训练的保障与评估等方面还面临着许多困难，加强与之相关的针对性研究，是确保训练顺利实施，最终形成复杂电磁环境下一体化作战能力的重要保证。

**关键词：**复杂电磁环境；电子对抗部队；一体化训练

为适应复杂电磁环境下一体化联合作战的需要，电子对抗部队开展复杂电磁环境下一体化训练势在必行，但面对这一新情况、新课题，我们没有现成的模式和方法可以遵循，只有瞄准实战需求和实际困难做好针对性研究，才能确保训练工作顺利实施和一体化作战能力的形成。

## 1 开展复杂电磁环境下一体化训练是电子对抗部队面临的现实课题

进行复杂电磁环境下针对性训练是适应信息化战场环境的必然要求。开展一体化训练是形成一体化联合作战能力、赢得一体化联合作战胜利的根本途径。电子对抗部队是夺取未来信息化战场制电磁权和制信息权的核心力量，开展复杂电磁环境下一体化训练是电子对抗部队面临的现实而紧迫的课题。

### 1.1 复杂电磁环境是对电子对抗部队作战行动影响最深刻的战场环境

复杂电磁环境，是指在一定的空域、时域、频域上，电磁信号纵横交叉、连续交错、密集重叠，功率分布参差不齐，对相应的电磁活动产生重大影响的电磁环境。电子对抗是作战双方使用多种电子对抗装备在电磁领域针对制电磁权展开的激烈争夺，它是战场电磁环境复杂化的重要原因，也受战场复杂电磁环境的深刻影响。因为各种电子设备的正常运行依赖于有效的电磁管控和频谱分配，信息

化战场上用频装备的急剧增加致使有限的电磁资源显得十分拥挤，电磁管控异常困难，外部电磁干扰威胁巨大和系统内部自扰、互扰问题突出，已严重制约了各型电子对抗装备作战效能的发挥。

### 1.2 开展一体化训练是电子对抗部队适应一体化联合作战的根本途径

作战样式决定训练方式，仗怎么打，兵就要怎么练，是组织军事训练必须遵循的基本规律。一体化联合作战是联合作战在信息化条件下发展的高级阶段，是我军未来最主要的作战样式，具有联合作战和信息化作战的双重特征，它强调开发和利用信息的作战潜能，形成和运用信息主导下的一体化联合作战力量，实施精确、高效、快速决定性的联合作战行动，实现由“信息优势——决策优势——行动优势”的转变。电子对抗部队作为信息时代一体化联合作战体系的最为重要的要素之一，只有有针对性地推进一体化训练，才能实现电子对抗力量内部的要素融合、单元融合，以及与一体化联合作战力量间的体系融合，形成强大的一体化联合作战能力。

### 1.3 开展复杂电磁环境下一体化训练是电子对抗部队的必然选择

随着电子信息系统和武器装备应用的日趋广泛，复杂电磁环境作为信息化战场最重要的环境构成因素之一，对未来作战和训练都将产生极其深刻的影响，同时，在复杂电磁环境下进行一体化联合

作战是我军未来无法回避的历史任务。在平时进行复杂电磁环境下一体化联合作战的针对性训练,是有效应对复杂电磁环境影响和增强部队一体化联合作战能力的根本途径。在信息化战场上,获取信息优势、夺控制信息权是赢得战场主动权的必要前提,而制信息权的实质就是制电磁权,电子对抗部队作为电磁领域斗争的主要力量,惟有搞好针对性的训练才能胜任这一历史重任。因此,开展复杂电磁环境下一体化训练,是电子对抗部队适应未来一体化联合作战的必然要求,也是电子对抗部队必须面对的现实课题。

## 2 当前开展复杂电磁环境下电子对抗部队一体化训练面临的困难

当前,电子对抗部队开展复杂电磁环境下一体化训练还面临着不少困难,主要体现在对复杂电磁环境的认知、训练内容的确定、训练方法的运用、训练环境的构建和训练效果的评估等方面。

### 2.1 对复杂电磁环境的认知有待深化

复杂电磁环境是由自然界电磁辐射、民用电磁辐射、己方军用电磁辐射和敌方实施的电磁干扰等多种因素综合作用形成的,它散布于时域、空域、频域、能域等广阔而无形的电磁空间,是未来信息化战场环境的重要组成部分,也是对信息化作战行动影响最为深刻的战场环境因素。通过研究,人们对复杂电磁环境已有了初步的认识,例如在复杂电磁环境的成因、构成要素、对作战与训练的影响等方面,形成了大量的理论成果,但由于复杂电磁环境具有很强的动态性,随着电子信息系统和技术装备的大量应用,它的复杂性、展现形态和影响程度等都会出现新的变化。因此,我们还必须深化对复杂电磁环境,尤其是它对信息化作战行动的影响及对策的认知研究。

### 2.2 训练内容确定难

电子对抗部队开展复杂电磁环境下一体化训练的内容体系,必须按照未来复杂电磁环境下一体化联合作战的要求来设置。目前,复杂电磁环境对一体化电子对抗行动产生的影响还没有完全弄清,电子对抗部队需要重点增强的能力也没有完全界定,

以及训练内容发展的动态性特征,致使复杂电磁环境下电子对抗部队一体化训练的内容体系难以科学确定。

### 2.3 训练方法不完善

电子对抗部队开展一体化训练的时间较短,还没形成完整的训练方法体系。尽管我们已经开始进行复杂电磁环境下军事训练实践的探索,一体化训练也在各军兵种部队展开,并积累了一些组训经验,但基于电子对抗部队受复杂电磁环境影响大、攻防主体分离等特殊性的,这些经验并不能完全满足电子对抗部队开展复杂电磁环境下一体化训练的需要,必须加强对训练方法探索。

### 2.4 训练环境需构建

复杂电磁环境作为一种客观存在,与其他战场环境因素相比,具有鲜明的无形性特征,使部队难以通过有限的手段将其对作战的影响尽显于训练中,即使进行模拟,也不能尽数显示信息化战场的逼真复杂电磁态势,部队训练系统与电磁环境得不到有效的关联,容易导致军事训练因复杂电磁环境产生的影响得不到充分体现而“失真”。因此,必须着力构建电子对抗部队复杂电磁环境下一体化训练的训练环境,这是确保训练质量的基础和前提。

### 2.5 训练效果评估难

对复杂电磁环境下军事训练评估,目前还没有具体评判标准和指标体系,此外,对不同的对象,复杂电磁环境的影响影响程度也各有所异,实践中很难用一个恰当的指标对其进行统一界定,对训练效果进行科学准确评估的难度较大。

## 3 电子对抗部队搞好复杂电磁环境下一体化训练的几点对策

搞好复杂电磁环境下电子对抗部队一体化训练,必须坚持训战一致、信息主导、整体筹划、求实创新、滚动发展的原则,从实际的困难和问题出发,以实战为标准,以实效为目标,以练指挥、练协同、练保障为重点,按照转变观念、健全体系、完善机制、创新训法、搞好保障的基本思路做好各

项工作。

### 3.1 转变观念，提高三个认识

电子对抗部队开展复杂电磁环境下一体化训练，首先必须解决思想准备和理论准备方面的问题，具体来说就是要提高三个认识：一是提高对开展复杂电磁环境下电子对抗部队一体化训练重要性的认识，解决思想不重视的问题；二是提高对开展复杂电磁环境下电子对抗部队一体化训练紧迫性的认识，解决行动不及时的问题；三是提高复杂电磁环境对未来电子对抗作战行动影响的认识，加强相应的对策研究，解决理论准备不充分的问题。

### 3.2 瞄准实战，确定内容体系

确定复杂电磁环境下电子对抗部队一体化训练内容体系，必须强调以未来一体化联合作战需求为核心，以形成满足作战需求的功能系统和强大的一体化电子战能力为目标。据此，确定以下训练内容：

#### 3.2.1 情报信息要素训练

重点解决复杂电磁环境下情报信息的获取、筛选、分析、处理和分发问题。包括复杂电磁环境下多元情报获取训练、信息组网训练、联合协作训练等。

#### 3.2.2 指挥控制要素训练

重点解决复杂电磁环境下电子对抗行动的指挥控制问题，提高对电磁频谱的管控能力。包括战场电磁态势认知训练，动态实时控制训练，分布式电子对抗指挥训练等。

#### 3.2.3 电子进攻要素训练

重点训练在复杂电磁环境下对敌实施电子干扰和反辐射打击、电子信息系统瘫痪等内容，增强电磁优势夺控能力。包括电子进攻力量的一体化联动训练，优化重组和快速联合打击训练，软硬一体复合打击训练等。

#### 3.2.4 电子防护要素训练

围绕提高整体电磁防护能力，各种电子信息系统的交互能力、抗毁能力和再生能力，重点进行复杂电磁环境下反敌电子侦察、电子干扰和实体摧

毁，防敌黑客攻击、信息欺骗、信息阻塞、渗透破坏等训练。

#### 3.2.5 综合保障要素训练

电子对抗综合保障训练的目标是实现作战、后勤、装备保障一体化，以适应未来实时、精确、动态和可视化战场保障的需求。包括模块保障训练、区域保障训练、联网保障训练和精确保障训练等，在复杂电磁环境下，尤其需要加强用频保障的训练。

#### 3.2.6 诸要素综合集成训练

要素综合集成训练是一体化训练的关键环节，是实现要素间横向融合、一体联动，提高复杂电磁环境下的整体电子对抗作战能力的重要途径。包括情报信息与指控要素融合训练，情报信息、指挥控制与电子攻防要素的融合训练和全要素综合集成训练。

#### 3.2.7 参与一体化联合作战体系融合训练

电子对抗作为制信息权斗争的核心力量，只有融入一体化联合作战体系，才能实现一体化联合作战信息作战目标。因此，在平时的训练中，就应该重视电子对抗力量要素与其他联合作战力量间的整体融合训练，重点解决用频协同的问题，以形成复杂电磁环境下强大的一体化联合作战能力。

### 3.3 着眼实效，完善训法体系

科学的训练方法是训练规律的反映，正确选择和运用复杂电磁环境下一体化训练的方法，对于提高训练质量、完成训练任务具有重要意义。对电子对抗部队来说，组织复杂电磁环境下的一体化训练不能急于求成，而要以完成训练任务、提升训练的实际效果为目标，理清思路，深入研究，按照循序渐进、先分后合、逐步集成的思路，把复杂电磁环境简单化，把无形的电磁态势可视化，科学合理地组织训练。一是将复杂电磁环境的相关理论融入到基础训练中，提高受训人员对复杂电磁环境的认知和掌握程度，奠定坚实的理论基础。二是按要素集成、单元集成和体系集成的步骤实施，增强复杂电磁环境下电子对抗部队的一体化作战能力。三是采用网络化、基地化、模拟化等多种手段，把基地化训练作为实施复杂电磁环境下训练的基本途径，通

过模拟出逼真的电磁训练环境,增强训练的针对性和实战化程度。四是强化复杂电磁环境下一体化对抗训练。要适应复杂电磁环境下一体化联合作战的需要,必须把复杂电磁环境下一体化对抗训练作为重要“抓手”,真正认识和把握战场电磁环境态势变化规律,看到复杂电磁环境对电子对抗作战行动的巨大影响,寻找在复杂电磁环境下作战的制胜之道。

### 3.4 立足实际,搞好综合保障

综合保障既是一体化训练的重要内容,也是维系训练顺利实施的根本保证,组织复杂电磁环境下一体化训练,必须做好训练环境设置、训练手段准备、训练管控和训练评估等各方面的保障工作。一是依托基地构建复杂电磁训练环境。组织复杂电磁环境下一体化训练,首先必须构建逼真的训练环境,从当前我军的实际情况来看,依托基地实施构建是形成复杂电磁训练环境的最佳途径。二是不断

创新训练手段。应用网络化、模拟化、虚拟化等先进的信息技术手段,是信息化条件下军事训练的特质和基本趋向。电子对抗部队开展复杂电磁环境下一体化训练,也应完善训练的信息网络,力求在网络化训练、模拟化训练和虚拟化训练中寻求突破。这些先进的训练手段,既可大大增强训练的针对性,提高训练效果,又能节约财力和物力,克服训练效果评估和成绩评判的随意性。三是建立健全科学高效的训练管控评估机制。训练管控,是指对训练进度和训练难度的管理调控,它和科学高效的训练评估一起构成准确调控训练进度、确保训练质量的重要保证。建立健全复杂电磁环境下电子对抗部队一体化训练管控评估机制,有助于各作战单元、作战要素围绕各自的目标展开训练,对训练目标的实现程度作出明确评价,科学调配训练时间,把握训练进度,并及时协调有关事项,确保训练效益的落实和训练的顺利实施。

### 参考文献

- [1] 王汝群等. 战场电磁环境[M]. 北京: 解放军出版社, 2006.08
- [2] 陈勇、杨业利主编. 试论一体化训练[M]. 北京: 军事科学出版社, 2004.05
- [3] 纪思办. 积极推进军事训练的历史性转变[J]. 北京: 解放军报第5版 2006.08.15
- [4] 熊作明. 复杂电磁环境下训练应重点解决的问题[J], 《指挥学报》2007(6)

### 作者联系方式

通信地址: 安徽省合肥市黄山路460号电子工程学院研三队  
邮政编码: 230037  
联系电话: 13696515543

## 第 6 部分

# 军队信息化建设关键技术

# 军用认知网络技术及其应用研究

王金龙 吴启晖 宋 绯

**摘 要:** 本文针对现有通信网络的不足, 着眼军事斗争准备, 围绕网络认知性及其环境感知、数据挖掘、智能决策以及网络可重配置等关键技术, 对认知网络的基本概念及其在军事通信网中的应用进行了阐述。

**关键词:** 认知网络; 智能决策; 环境感知; 数据挖掘; 网络可重配制

## 1 引言

近年来, 随着信息技术的进步和获取战场信息的需要, 美国等发达国家正在开发适于未来战场需要的军用通信网络系统。2003 年, 从事高尖端军事设备开发的美国雷声公司从美国国防部 (DARPA) 手中接下了有关研发美军下一代无线 (XG)<sup>[1]</sup> 通信计划的合同。该计划的目标是利用认知无线电技术, 全面解决机会频谱访问问题。面对复杂的战时环境, 我军现有的通信网络缺乏对战场环境的认知能力、网络参数可重配置能力以及自身动态调整的智能决策能力。正因为缺乏这些能力, 使得我军通信网络不能随着外部环境的变化进行动态调整。比如由于不具有频谱认知能力, 我军仍然采用静态、集中式的频谱管理机制, 不能够适应外部电磁环境的快速变化。

综上所述, 认知能力对于我军新一代通信网络至关重要。我们需要将它作为新一代军事通信网络的基础进行重点研究, 以全面提升军事通信网络的环境自适应、动态频谱规划、智能抗干扰等能力。

## 2 基本概念

认知网络<sup>[2][3]</sup>是指网络能够感知外部环境, 通过对外部环境的理解与学习, 实时调整通信网络内部配置, 智能地适应外部环境的变化。

军用认知网络是指通信网络能够感知战时环境, 通过对战时环境的理解与学习, 实时调整通信网络内部配置, 智能地适应战时环境的变化。其内涵主要体现在下列三个方面。

1) 从通信网络这一主体所处的外部环境来看

是战时环境。战时环境与和平环境有很大区别, 针对通信网络而言, 其区别主要体现在电磁环境复杂、作战信息量剧增、对抗力度超强等方面。

2) 从通信网络这一主体强调的能力来看是认知能力以及自我配置能力。采用认知无线电等技术, 实现“感知—决策—行为”的动态自适应过程。主要包括感知、决策、行为。

3) 从通信网络主体本身来看是一体化的通信网络。它包括了各种战时通信网络, 甚至战时征用的民用通信网络。

## 3 认知网络理论体系

图 1 给出了认知网络的理论体系。该理论体系从人类的认知特性出发, 以系统工程方法论、信息处理与人工智能为基础, 围绕认知将环境感知、数据挖掘、智能决策与网络动态配置紧密有机地结合在一起。

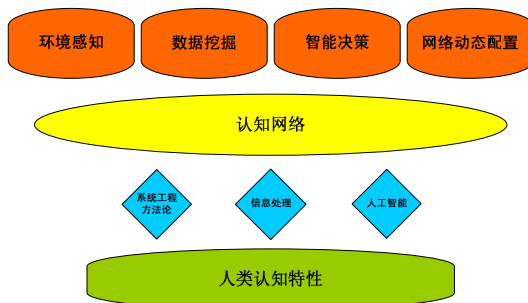


图1 认知网络理论体系

在认知网络理论体系中, 环境感知、数据挖掘、智能决策与网络动态配置存在紧密地内在逻辑性, 其关系如图 2 所示。环境感知包括对无线环境与网络环境的感知。环境感知为数据挖掘提供基



础，而数据挖掘为智能决策提供依据。智能决策确定了网络重构的具体目标。网络重构的实施使得网络能够动态适应环境。

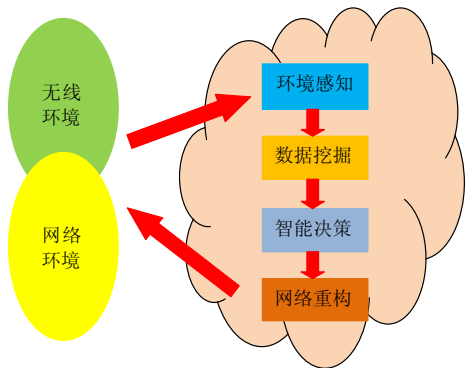


图2 理论体系内在逻辑关系

4 关键技术

认知网络所要研究的核心科学问题主要包括：环境分析及感知、环境自适应理论研究及其组织运用理论研究等。其关键技术包括：环境感知技术、数据挖掘技术、智能决策技术、网络可重配置等。

4.1 环境感知技术

环境感知是实现通信网络认知的基础，所要感知的内容包括无线环境与网络环境。无线环境感知的主要研究内容有：无线环境的分析，包括对无线传播环境干扰度（interference temperature）的估计以及频谱空穴（spectrum holes）的检测；信道的确认，包括对信道状态信息的估计以及对信道容量的预测；发射功率控制及动态频谱管理等。频谱空穴检测是目前研究的重点，其主要方法有循环谱检测法等。

网络环境感知<sup>[4]</sup>是网络环境自适应的基础。研究内容包括网络环境信息的获取、表示、融合和利用。其中，网络环境主要包括网络类型、网络拓扑、接口协议、可用资源、网络流量等影响端到端传输性能的网络工作状态。迅速准确地感知网络环境的变化，及时调整网络配置是充分发挥多种传输手段综合效能，保证未来信息化战场信息可靠传输的关键环节。

4.2 数据挖掘

数据挖掘就是从大量的、不完全的、有噪声的、模糊的、随机的实际应用数据中，提取隐含在

其中的、人们事先不知道的、但又是潜在有用的信息和知识的过程。这个定义包括好几层含义：数据源必须是真实的、大量的、含噪声的；发现的是用户感兴趣的知识；发现的知识要可接受、可理解、可运用。

应从环境特征分析入手，重点研究数据挖掘五大功能：自动预测趋势和行为，关联分析，聚类，概念描述，偏差检测。环境特征分析包括两个方面与两个层次，两个方面是指无线环境特征分析与网络环境特征分析，两个层次是指认知节点与网络。数据挖掘充分体现区域性与面向决策性。通过数据挖掘理论与算法的研究为智能决策提供依据。

4.3 智能决策

智能决策是利用人工智能，特别是专家系统的原理和技术所建立的辅助决策的计算机软件系统，支持半结构化和非结构化问题的决策。智能决策系统主要包括决策支持系统、专家系统、机器学习、效能评价等。军用认知网络是一个具有智能的主体，我们将人工智能理论、机器学习、推理机制引入军事通信网络决策系统，使得军用通信网络能够实现环境自适应。

目前博弈论是研究的热点之一。博弈论，就是使用严谨数学模型来解决现实世界中的利害冲突的理论，又称对策论。它被设计用来帮助我们理解所观察到的决策主体相互作用时的现象。这种理论隐含的基本假设是：决策主体追求确定的外部目标（他们是理性的）并且考虑他们自身的知识或其他决策主体行为的期望。博弈分好几种。S 模（S-modular）博弈分为超模（Supermodular）博弈和副模（Submodular）博弈两种。图 3 给出了博弈在无线资源管理中的应用。

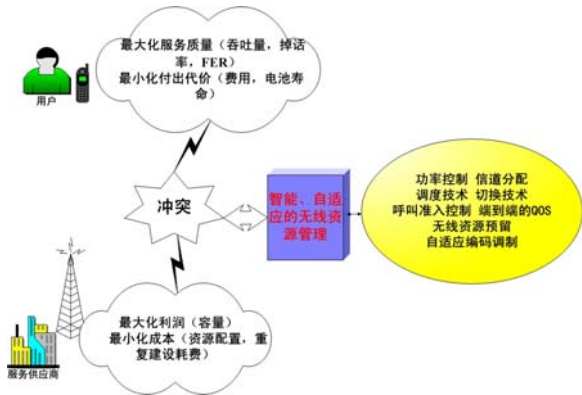


图3 无线资源管理应用图



除了要将无线资源管理博弈论拓展到网络配置决策,我们还需研究智能决策的性能评价机制,根据环境分析的结果和用户输入判断决策结果是否最优,来调整网络认知循环的各个环节。

#### 4.4 网络可重配置

目前的网络配置和管理有很多是依赖人工,无论是网络建设的初期还是后期的维护,这将极大的增加网络的配置和维护成本,而且其配置效果常不理想,系统的整体性能欠佳。按照未来异构网络的特征,各个网络在网络拓扑、工作模式还是设备参数上,都会动态变化,过分依赖人工的配置和管理显然已不再适用。总之,未来具有认知网络应具备自配置、自管理、自优化功能。这就需要网络的可重配置特性。

针对网络可重配置,将沿着这样的思路进行研究。从认知网络体系结构出发,研究网络可重配置体系、网络可重配置元与快速配置设计。由于认知网络具有动态、灵活、智能、重配置的特征,因而对网络协议的要求也比较高,要求协议具有异步、实时的特点,必须能自适应于因终端变动、环境变动而带来的网络资源的动态变化、网络拓扑结构的改变。因此,在网络体系结构必须考虑重配置功能,协议设计应充分反映认知无线电技术的特征,协议架构设计应结合算法与网络结构设计的成果进行系统性地考虑,网络体系结构需支持智能的控制与管理。

为了支持网络可重配置特性,网络可重配置元研究已经提上日程。网络可重配置元初步设想如图4所示。

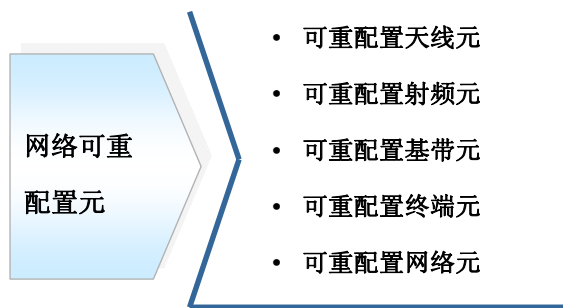


图4 网络可重配置元

快速配置设计研究从跨层设计入手,跨层设计可以对分散在网络各子层的特性参数进行协调融合,以优化网络整体性能。

## 5 应用研究

### 5.1 电磁频谱管控技术

频谱管理在民用方面主要是保证民用通信链路的稳定,在军用研究中旨在结合我军战时电磁频谱管控的实际需求,综合考虑复杂战场环境通信、通信对抗等装备或系统组织运用情况,通过对区域电磁频谱管控功能可重构技术体制、DBF可重构天线技术、复杂战场环境电磁频谱动态预测与效能评估方法等新概念、新原理、新体制和新技术的深入研究,发展综合一体化的新型电磁频谱管控装备,有效解决战场电磁兼容性问题,获得战场电磁频谱优势。研究的重点在于区域电磁频谱管控功能可重构技术、DBF可重构天线技术、复杂战场环境电磁频谱动态预测与效能评估方法等。

### 5.2 智能抗干扰

在通信对抗、抗干扰通信、认知无线电等理论研究的基础上,提出智能抗干扰通信理论与机制。智能抗干扰来源于通信对抗机理与通信抗干扰理论的联合研究,通过对这两者的研究,分析了各种干扰模式下的抗干扰方法,研究出一些新的抗干扰机制。例如针对跟踪式干扰,采取更换新的频率集的方法来获取干扰时隙;针对部分频带阻塞式干扰,采用选频点的方式。

智能抗干扰的基本机制是:①通过信道质量估计来判定通信是否受到干扰,若没有受到干扰,则保持现有工作状态;若有干扰,则进行干扰环境特征识别;②通过频谱感知与信道质量感知及特征提取,确定所处的电磁环境与所采取的抗干扰策略;③通过可靠信令将控制命令传递到发方,使收发工作一致。智能抗干扰机制示意图如图5所示。

### 5.3 自适应天基网络

战时环境自适应天基网络能够根据当前可用卫星资源自动组网,实现网络和通信结点的自愈,并能利用所有可用卫星实现协同通信。该系统综合利用了GEO和NGSO通信的多层卫星通信网,各通信卫星之间采用星际链路互连,用户终端能够利用不同类型的卫星进行通信,从而构成一个立体的天基网络。其研究重点在于多层卫星网自组织技术、卫星通信平台可重构技术、卫星通信中的协同通信技术。

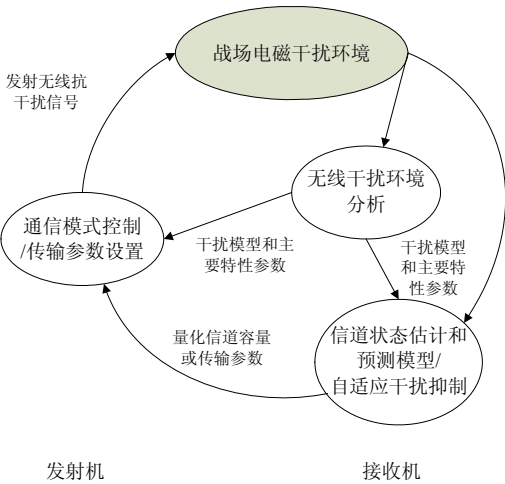


图 5 智能抗干扰机制示意图

## 6 结论

面向军事斗争准备的需要及军用环境，以环境自适应研究为中心，本文提出了军用认知通信网络的概念，并分别对其关键支撑技术以及组织应用进行了阐述，该网络是下一代军用通信网络的可行方案之一，具备环境认知及自适应能力，能在复杂环境下为战场电子信息系统提供必要的网络和服务支持；增强集散节点和集群结构网络对抗蓄意攻击和破坏的能力；全面提升通信网络安全防护、电磁防护、物理防护能力；实现资源共享，发挥整体效能。

### 参考文献（略）

### 作者联系方式

通信地址：南京市御道街标营 2 号通信工程学院  
邮政编码：210007  
联系电话：025-80828001

# 矩型码——一种适合地下通信的纠错检错码

司徒梦天 宁志德 方家喜

**摘 要：**本文介绍一种码组长度可变的纠错检错码——矩型码。首先介绍矩型码的结构，然后介绍其纠错及检错的原理及计算方法，最后与 RS 码进行比较，并说明它特别适合地下通信“短信息”、“高可靠”的要求。

**关键词：**纠错编码；差错控制；地下通信

## 1 地下通信的特点

地下通信是收发信设备及天线全部设置在地下的无线电通信，具有“隐蔽”、“抗毁”的突出优点，在军事上是一种有效的“抗毁应急通信手段”。

由于天线设置在地下，电波需穿透岩层传播，衰减十分严重，使得接收信号十分微弱，因此信息速率极低，通常只用来传递一些最紧急、最重要的短信息，以确保通信指挥的不间断。由于这些信息是最紧急、最重要的，如导弹打击目标指令等，因此要求错误概率极低，即十分准确可靠。“短信息”、“高可靠”这就是我们考虑差错控制技术的两个出发点。

## 2 差错控制方式的确定

由于要求差错率极低，因此仅用前向纠错（FEC）难以满足要求。众所周知，码组的检错能力总是高于纠错能力的。因此因优先考虑混合纠错方式（HEC），能纠的就纠，超过纠错能力的就检，然后反馈重传。

## 3 纠错码的考虑

纠错码分为两大类：① 是卷积码，通常适用于 FEC，不适合反馈重传（ARQ），故不采用。② 是分组码，既适用于纠错，也适用于检错。但分组码的码组长度固定，对于短信息需要填 0 以凑足编码长度，使传信率大大降低。RS 码是公认的、性能优良的多元制纠错编码。但码组长度是

15 位。对于通信速率极低、发送报文短且长度可变的情况（如地下通信，只发送 4 位信息），若用 RS 码就必需填 0，使码组凑够 15 位，是很不合算的。为此我们提出了一种能较好地适应上述情况的纠错编码方式——短信息、高可靠的矩型码。

## 4 矩型码介绍

### 4.1 矩型码的结构

将待发字符排成矩阵如图 1 所示，矩阵的行数为 A，列数为 B，每行加校验码 K，K 为 0~F 中的某一字符，K 值的选取应使该行字符模 16 加为 0，例如图 1 中的矩阵第一行为 F 5 3 A，则 K 值应为 F。（因  $15+5+3+10+15=48$ ， $48 \bmod 16=0$ ）。同理，第二行的校验码为 6，第三行的校验码为 5。此外每列也加校验码，如矩阵的第一列的校验码为 9，第二列的校验码为 F 等等，最后，校验行 9F4E 也加校验码，如本例为 6，可以证明，此码也是校验列 F65 的校验码。下面我们将分别研究“矩型码”的纠错与检错性能，并与 RS 码进行比较。

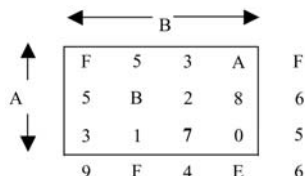


图 1 矩型码的结构

### 4.2 矩型码的纠错能力

将图 1 所示的矩型码发送到收方，收方进行校验，即对每行、每列都进行模 16 加。若传输无误，则校验结果均应为 0。若传输有误，如第一

行、第二列的 5 错成 6，错误增值为+1，如图 2 所示，则第一行和第二列的校验结果都为+1，于是将此位置的 6 减去 1 得 5，即可将错误纠正。

F	<u>6</u>	3	A	F	+1
5	B	2	8	6	0
3	1	7	0	5	0
9	F	4	E	6	0
0	+1	0	0	0	

图2 第一行、第二列的 5 错成 6 的校验结果

根据矩型码纠错的原理，容易得出以下结论：错 1 码必能纠。  
在错 2 码的情况下，大多数也能纠，例如，除上述 5 错成 6 之外，第 3 行、第 3 列的 7 错成 4，错误增值为-3，如图 3 所示。

F	<u>6</u>	3	A	F	+1
5	B	2	8	6	0
3	1	<u>4</u>	0	5	-3
9	F	4	E	6	0
0	+1	-3	0	0	

图3 错 2 码的校验结果

此时，除了将第一行、第二列的 6 减 1 外，再将第 3 行、第 3 列的 4 加 3，即可将错误纠正过来。错两个码不能纠的情况有两种，一种情况是：错误的两码发生在同一行（或同一列）上，且其错误增值互补，如图 4 所示（图中显示的是误码增值）。另一种情况是：错误的两码既不在同一行，也不在同一列，但其错误增值相同，如图 5 所示。

	+3		-3	0

图4 两码错在同行且错误增值互补，就不知哪行有错

	+4		?	+4
	?		+4	+4

图5 两错码既不同行也不同列且错误增值相同，就无法确定错误位置

于是在错两码的条件下：  
第一种不能纠的概率是：（两错码同行或同列的概率）×1/15

某 16 元字符错成其他字符的样式有 15 种，而其中只有一种能满足增值互补的要求。因此 1/15 是错误增值互补的概率。

第二种不能纠的概率是：（两错码不同行也不同列的概率）×1/15

1/15 是错误增值相同的概率。这两种不能纠的概率之和，就是错两码时不能纠的概率。它等于：（两错码同行或同列的概率+两错码不同行也不同列的概率）×1/15=1/15

于是错两码能纠的概率为 1-1/15=14/15。容易证明，错 2 码总是必定能检的。

有时错 3 码也能纠，但此概率很低，就不予考虑了。

当我们只采用前向纠错（FEC），根据以上分析，就可以推导出信道误码率 P 和 A×B 矩型码组错误率的关系。现推导如下：

A×B 矩型码的码组长度 n=（A+1）（B+1）。码组正确接收概率以 P<sub>ZC</sub> 表示。

$$P_{ZC} \geq (n \text{ 个码全对的概率}) + (\text{错 1 码的概率}) + (\text{错 2 码的概率}) \times 14/15$$

上式中采用≥符号是因为错 3 码或错 3 码以上有时也能纠，而我们将它略去。

根据贝努利定理即可得：

$$P_{ZC} \geq (1 - P)^n + C_n^1 P(1 - P)^{n-1} + C_n^2 P^2(1 - P)^{n-2} \times 14/15 \tag{1}$$

码组错误率 P<sub>ZE</sub>≤1-P<sub>ZC</sub>

【计算举例】发送 4 个字符，加校验后成 3×3 矩阵，n=9。设信道误码率 P=0.01，计算纠错后矩型码码组的错误率。

以 P=0.01，n=9 代入（1），得：

$$P_{ZC} \geq (0.99)^9 + 9 \times 0.01 \times 0.99^8 + 36 \times 0.01^2 \times 0.99^7 \times 14/15 = 0.999696$$

$$\text{矩型码误组率 } P_{ZE} \leq 1 - P_{ZC} = 3.04 \times 10^{-4}$$

4.3 矩型码的检错能力

矩型码的检错能力极强，前已分析过，矩型码错 2 码必能检。当误码数为 3，且出现在矩形的顶上，并且增值互补时，才不能检（还产生误纠），如图 6 所示。而这种概率是极低的。

不但能检，且误认为！位置的增值为-5 而误纠错 4 个码，且错在矩形的顶上，其增值又互补，如图 6 中！位置上的误码增值为+5，由于此时所有校

验结果都为 0, 也不能检。但其概率更低, 将不予考虑。

+5	-5	0
-5	!	-5
0	-5	

图 6 3 个错码发生在矩形的顶上且增值互补时不能检

根据上面分析, 在错 3 码条件下不能检的概率为:

$$P_D \times 1/225$$

上式中  $P_D$  为 3 个错码位于矩形顶点的概率。

$$P_D = A(A+1)B(B+1)/C_n^3 \quad (2)$$

$1/225 = 1/15 \times 1/15$  为错码增值互补的概率。

于是在错 3 码条件下仍能检的概率为:  $1 - P_D \times 1/225$

下面先计算采用矩型码进行纠错和检错技术后, 码组正确接收的概率  $P_{ZC}$ 。这里假设检出错误后经重传, 就可将错误纠正。若重传还有错, 则再进行反馈重传。出错的原因只是因为遇到了不可检测的错误样式。

$P_{ZC} \geq (\text{n 个码全对的概率}) + (\text{错 1 码的概率“必能纠”}) + (\text{错 2 码的概率“必能检”}) + (\text{错 3 码的概率}) \times (1 - P_D \times 1/225 \text{ “能检”})$

上式中用  $\geq$  是因为错 4 码或 4 码以上的错误也可能检出, 并通过反馈重传加以纠正, 但其概率更低而在上式中未加考虑。根据贝努利定理即得:

$$P_{ZC} \geq (1-P)^n + C_n^1 P(1-P)^{n-1} + C_n^2 P^2(1-P)^{n-2} + C_n^3 P^3(1-P)^{n-3}(1-P_D/225) \quad (3)$$

码组错误率  $P_{ZE} \leq 1 - P_{ZC}$

**【计算举例】**发包含 4 个字符的命令代码, 加校验后  $n=9$ 。设信道误码率  $P=0.01$ , 计算纠错和检错后矩型码码组的错误率。

$$P_D = 2 \times 3 \times 2 \times 3 / (9 \times 8 \times 7) / (3 \times 2) = 3/7$$

将  $n=9; P=0.01; P_D=3/7$  代入 (3) 得  $P_{ZC} \geq 0.999998639$ 。

于是得: 矩型码误组率  $P_{ZE} \leq 1 - P_{ZC} = 1.36 \times 10^{-6}$

## 5 矩型码和RS码的比较

RS 码是极大最小距离码, 即最小距离  $d=r+1$ ,  $r$  是校验元的个数, 它能纠  $t \leq (d-1)/2$  个错误和检  $e \leq d-1$  个错误。RS 码是一种公认的性能优越的

多进制 BCH 码。在 16 元移频键控中 RS 码的分组长度  $n=2^4-1=15$ 。信息元为  $k$  位, 监督元为  $r$  位, 其中  $r=n-k$ 。

(1) 在码元长度相同的条件下进行比较, 此时二者的信道误码率  $P$  是相同的

1) 下面, 先选码组长度最接近 15 的矩型码来和 RS 码进行比较。为此, 矩型码取信息元  $k=3 \times 3=9$ , 加上监督元组成  $4 \times 4$  矩阵, 于是矩型码码组长度  $n=16$ , 它比较接近 15。RS 码同样取  $k=9$ , 则  $r=6$

通信速率的比较:

RS 码的码率是  $9/15=0.6$

矩型码的码率是  $9/16=0.5625$ 。RS 码略优于矩型码, 通信速率比为 1.07。

纠错能力的比较:

RS 码能纠 3 个以下的错误, 码组正确接收概率为:

$$P_{ZC} = (1-P)^{15} + 15P(1-P)^{14} + 105P^2(1-P)^{13} + 455P^3(1-P)^{12} \quad (4)$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.9999875$  误组率  $P_{ZE}=1.25 \times 10^{-5}$

以  $n=16$  代入 (1) 可得矩型码经纠错后码组的正确接收概率:

$$P_{ZC} = (1-P)^{16} + 16P(1-P)^{15} + 120P^2(1-P)^{14} \times 14/15$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.998797$  误组率  $P_{ZE}=1.203 \times 10^{-3}$

检错能力的比较:

RS 码能检 6 个错误, 经反馈重传后, 码组正确接收概率为:

$$P_{ZC} = (1-P)^{15} + 15P(1-P)^{14} + 105P^2(1-P)^{13} + 455P^3(1-P)^{12} + 1365P^4(1-P)^{11} + 3003P^5(1-P)^{10} + 5005P^6(1-P)^9 \quad (5)$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.99999999994$  误组率  $P_{ZE}=6 \times 10^{-11}$ 。

矩型码经检错及反馈重传后, 根据 (3) 式码组的正确接收概率约为:

$$P_{ZC} = (1-P)^{16} + 16P(1-P)^{15} + 120P^2(1-P)^{14} + 560P^3(1-P)^{13}(1-P_D/255)$$

$$P_D = 3 \times 4 \times 3 \times 4 / C_{16}^3 = 0.257142857$$

$$P_{ZC} = (1-P)^{16} + 16P(1-P)^{15} + 120P^2(1-P)^{14} + 560P^3(1-P)^{13} \times 0.998857142$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.9999829$  误组率  $P_{ZE}=1.71 \times 10^{-5}$ 。

经比较可得如下结论。

**结论 1:** 在码元长度相同的条件下, RS (15, 9) 码, 与 A=3, B=3 矩型码比较, RS 码的通信速率略高于矩型码, 且 RS 码的纠错与检错能力远高于矩型码。

考虑传送长度极短且可变的报文情况, 如 4 个信息元和 2 个信息元, 可组成  $n=3 \times 3=9$  的小矩型码或  $n=3 \times 2=6$  的更小矩型码。而采用 RS 码则需填 0 以确保码组长度  $n=15$ 。下面比较 RS 码与 A=2, B=2; 和 A=1, B=2 小矩型码的性能。

2) RS 码与小矩型码比较通信速率比较:

A=2, B=2 矩型码  $n=9$ , 只需发 9 个码元, 而 RS 码必需发 15 个码元, 矩型码的通信速率为 RS 码的 1.7 倍。

A=1, B=2 矩型码  $n=6$ , 只需发 6 个码元, RS 码必需发 15 个码元, 矩型码的通信速率为 RS 码的 2.5 倍。

纠错能力的比较:

RS 码的纠错能力和以上分析的相同。因为其码的结构不变, 仅信息位以 0 补足。

A=2, B=2 矩型码经纠错后 码组的正确接收概率根据 (1) 式约为:

$$P_{ZC}=(1-P)^9+9P(1-P)^8+36P^2(1-P)^7 \times 14/15$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.999696$  误组率  $P_{ZE}=3.04 \times 10^{-4}$

A=1, B=2 矩型码经纠错后 码组的正确接收概率约为:

$$P_{ZC}=(1-P)^6+6P(1-P)^5+15P^2(1-P)^4 \times 14/15$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.9998844$  误组率  $P_{ZE}=1.156 \times 10^{-4}$

检错能力的比较:

RS 码的检错能力和以上分析的相同。因为其码的结构不变, 仅信息位以 0 补足。

A=2, B=2 矩型码经检错及反馈重传后, 码组的正确接收概率根据 (3) 式约为:

$$P_{ZC}=(1-P)^9+9P(1-P)^8+36P^2(1-P)^7+84P^3(1+P)^6(1-P_D/225) \\ P_D=2 \times 3 \times 2 \times 3/C_9^3=3/7$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.99999864$  误组率  $P_{ZE}=1.36 \times 10^{-6}$ 。

A=1, B=2 矩型码经纠错后码组的正确接收概率约为:

$$P_{ZC}=(1-P)^6+6P(1-P)^5+15P^2(1-P)^4+$$

$$20P^3(1-P)^3(1-P_D/225)$$

$$P_D=1 \times 2 \times 2 \times 3/C_6^3=3/5$$

当  $P=10^{-2}$  时,  $P_{ZC}=0.9999998$  误组率  $P_{ZE}=2 \times 10^{-7}$ 。

**结论 2:** 在码元长度相同的条件下

A=2, B=2 的矩型码通信速率为 RS 码的 1.7 倍;

A=1, B=2 的矩型码通信速率为 RS 码的 2.5 倍。

虽然矩型码的纠错、检错能力不如 RS 码, 但经 HEC 后, 已具有很低的误组率。当信道变差, 即便信道误码率下降了 2 个数量级使  $P=10^{-2}$ , 而 A=2, B=2 的矩型码误组率仍低于百万分之 1.36, A=1, B=2 的矩型码误组率则低于千万分之 2。

从以上计算还可以看出, 矩型码越小, 其纠错和检错能力越强 (即在相同的信道误码率条件下, 矩型码越小, 经纠错和检错后, 其误组率越低。) 这是因为矩阵越小, 编码效率越低, 即校验码所占的比例越大的缘故。

(2) 在通信速率相同的条件下进行比较

在通信速率相同的条件下进行比较, 更为科学合理。下面我们比较 RS 码和小矩型码 ( $n=9$ ) 的性能。当  $n=9$  时, 在通信速率相同的条件下, RS 码与矩型码的码元长度之比为  $9/15=0.6$ , 即码元能量相差  $10\log 0.6=-2.2\text{dB}$ 。经计算<sup>[1]</sup>信道误码率  $P=10^{-2}$  时 SNR 为  $-20\text{dB}$  (白噪声, 测量带宽  $2700\text{Hz}$ ) 若采用 RS 码并保持通信速率不变, 则 SNR 降低  $2.2\text{dB}$ , 即  $\text{SNR}=-22.2\text{dB}$ , 此时算得  $P=1.2 \times 10^{-1}$ 。

纠错能力的比较:

前已算得, 当信道误码率  $P=10^{-2}$  时,  $n=9$  的矩型码其误组率  $P_{ZE}=3.04 \times 10^{-4}$ 。

在通信速率相同的条件下, RS 码的码元能量下降  $2.2\text{dB}$ , 此时信道误码率  $P=0.12$ , 根据 (4) 式经纠错后, RS 码码组的正确接收概率为:

$$P_{ZC}=0.90414。于是得: 误组率 P_{ZE}=9.586 \times 10^{-2}$$

检错能力的比较:

前已算得, 当信道误码率  $P=10^{-2}$  时,  $n=9$  的矩型码其误组率  $P_{ZE}=1.362 \times 10^{-6}$

采用 RS 码, 在通信速率相同的条件下, 由于码元能量下降  $2.2\text{dB}$ , 此时信道误码率  $P=0.12$ , 经 HEC 后, 根据 (5) 式, 可算得: RS 码码组的正

确接收概率为。

$P_{ZC}=0.99904465$ 。于是得：误组率  $P_{ZE}=9.5535 \times 10^{-4}$

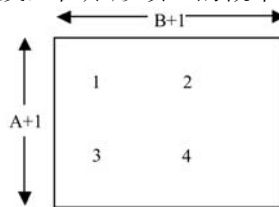
**结论 3：**在通信速率相同的条件下， $n=9$  的小矩型码，其纠错能力和检错能力，都比 RS 码约优 2 个数量级。

## 6 结束语

矩型码的矩阵大小可根据信息长度进行调整，避免了分组码码组长度固定，在传极短信息时需要填 0 以凑足编码长度，致使通信速率降低的缺点。由于矩阵大小可调，可以在信道差时将信息打成小包，即采用小矩阵来提高纠错和检错能力。小矩型码具有很强的检错能力，如信道误码率降到  $10^{-2}$  时， $n=9$  的码组错误率仍低于百万分之 1.36。 $n=2$  的码组错误率则低于千万分之 2。通过大量的实际通信试验，收到的信息都准确无误，证明了采用矩型码和 HEC，是一种适合地下通信的差错控制技术。

## 附录

3 个错码发生在矩形顶上的概率



附图的矩阵由  $n=(A+1)(B+1)$  个码元组成。错 3 个码的图样共有： $C_n^3$  种。

下面计算 3 个错误位于矩形顶上可能有多少种图样。

矩形顶分别以 1、2、3、4 表示。1、2 可能出现在第一行，也可能在第二行。共有  $A+1$  种可能，这两点在每行出现的位置又有  $C_{B+1}^2$  种组合。而第 3 个错码可能在 3，也可能在 4，即有 2 种可能。第 3 错码所处的行，又有  $A$  种不同可能。因此 3 个错码位于矩形顶上的图样共有：

$(A+1) C_{B+1}^2 \times 2 \times A = A(A+1)B(B+1)$  种；

于是，3 个错码发生在矩形顶上的概率为：

$$A(A+1)B(B+1) / C_n^3$$

## 参考文献

[1] 司徒梦天. 解决地下通信技术难题的方案及关键设备. 中国工程科学 2001 年 3 卷 7 期

## 作者联系方式

通信地址：北京丰台区大成路 13 号

邮政编码：100039

联系电话：010-66820010

# 谈大型作战方案解算

徐洸 陈建林

**摘 要：**本文首先分析了大型作战方案的模型特征和解算难点，然后具体介绍了大型作战方案解算的核心算法、前沿技术和非常规手段及其运用方法，最后探讨了集成各类解算方法和技术的综合解算体系。

**关键词：**作战方案；解算方法；数学模型；群集；人工生命算法；综合解算体系

大型作战方案是作战行动规模比较大，数学模型比较复杂，使用常规手段和经典算法难以迅速求解的作战方案。信息化战争中的空中进攻战役、首都联合防空战役、对敌航母编队的海空联合突击等大规模作战行动，其体系对抗特征明显，行动节奏快，制约作战行动和进程的因素非常复杂，在时效性和科学性方面对大型作战方案的制定提出了更高的要求，对传统的方案解算方法提出了巨大的挑战，应予以认真研究。

## 1 模型特征及解算难点

使用计算机对作战方案进行解算，必须将作战方案模型化，因此，对解算难点的分析，可以着眼模型特征展开。

### 1.1 主体模型多为大规模混合整数规划，解算时间过长

从运筹学的角度分析，用数学规划来定量描述作战方案较为科学，也最为自然。方案优劣的衡量标准直接对应于数学规划的目标函数，可用的兵力兵器及弹药等资源限制和任务要求则对应于数学规划的约束条件。结合方案变量的军事意义、变量集规模和部分变量的整数特征，就可以说，大型作战方案的模型主体多为大规模混合整数规划。

采用经典的算法和一般硬件手段解算一个规模为 40 个变量和 20 条约束的线性整数规划问题，用时约 1 秒。但随着变量数的增长，解算时间会迅速增加。分析最常用的分枝定界算法的寻优机制，以及实际解算用时的统计数据，可以发现，整数规划的解算用时随变量数的增长大致按几何级数的规律

延长。

### 1.2 模型体系内嵌多层非线性模型和规则，无通用精确算法

考察大型作战方案模型的内部结构，就会发现，模型体系又嵌套多层非线性模型，还有以阶跃函数、模糊函数等形式存在的规则集。对此类问题，目前尚无通用精确算法。

以空中进攻战役方案模型的目标函数为例，本身为非线性模型；同时，在计算构成目标函数的敌防空体系效能时，又要调用基于图论的计算模型；在计算敌我双方战损时，要调用多对多空战模型、空中突防和突击模型，从而形成非线性模型集。

非线性规划与非线性方程的解算方法和难度具有质的不同，是更大的难点。目前国际上最著名的解算工具，如 Maple 等，均未提供通用的全局寻优的精确算法。

### 1.3 模型变量中包含时间维变量，解算难度大幅度增加

在模型变量即方案结果数据中需包括时间维，原因在于：一方面，敌方目标体系中各个目标的地位不同，目标之间相互关联，要迅速实现瘫痪敌作战体系的目标，需要精心确定打击次序；另一方面，我方前面的作战行动效果将直接影响后续作战行动，作战行动必须前后衔接，要求科学区分行动波次，在方案要素中要包括时间维。

加入时间变量，会进一步强化模型变量间的关联，使问题转换为组合优化。在进行算法设计时，必须考虑这些多样化、不规则的行动间制约关系，从而将解算难度又提高了一个层次。



## 1.4 特殊模型形态不断出现，使经典解算方法无能为力

作战目标的弹性化，作战条件的随机性，导致在作战任务以及作战指挥原则中，有很多定性要求。如：“争取在第一突击波次取得战果”、“重点突击‘战略’目标”、“在敌方‘中度’干预条件下有把握截击绝大多数来袭兵器”等。与此类要求相适应，许多更特殊的作战方案模型形式不断出现，如随机规划、模糊规划等，对核心算法提出了特殊的要求，经典解算方法远不能适应。

## 2 解算方法和技术手段

通过对大型作战方案解算难点的分析，可以发现，大型作战方案模型的基本形式，是变量集中包括时间维且可能具有随机性和模糊性特征的大规模、非线性混合整数规划。它的解算，在时效性处理、复杂性处理、时序性处理和特殊性处理四个方面对经典的解算手段和技术带来了困难，必须积极寻求非常规和前沿的方法和手段。

### 2.1 高性能计算技术——网格与群集解算技术

网格与群集技术均属高性能计算技术，是应对大型作战方案的变量规模和解算时效性问题的有效手段。

网格解算。从方案解算的角度出发，可把网格抽象为一个部署在网络上的巨大的函数。我们可以用调用本地函数的模式调用它。例如：可将可用的兵力兵器数量、突击目标列表传给解算主机，网格主机上的远程函数进行解算，完成后将结果传给调用端，结果数据中包括目标选择、兵力分配、弹药使用、支援掩护力量、突防航线和突击次序等。网格解算有非常突出的优点：可以充分利用各类各档次的解算资源；服务器端的解算服务程序可以由顶级的算法专家与程序员完成和动态更新，基础数据和情报数据由有关机构维护；前端用户只需按规范调用而不用过问实现细节，可以像调看信息一样调用网上的计算能力，这是方案解算模式的一次重大变革。

群集解算。在有更高性能网络保障的条件下，更高效的解算技术是群集技术，这是一种将多台主

机整合成逻辑上的一台主机的技术。目前最方便使用的具体技术是.Net Remoting，即远程处理技术。它在主机间构建一种称为频道的信息通道，各机之间不仅可以传递形式化数据，还可以实时传递对象，从而以更高的水平将多台物理主机整合成逻辑上的单台主机，来提供非常规解算能力。下面举例说明群集的特殊解算策略：三台主机同时开始解算；当A主机发现第一个当前最优解后，迅速向群集广播；B和C主机寻优标准立即按梯次调高，去除无前途的搜索空间；当B主机发现新解的阶段最优解，再次进行广播，A和C主机的寻优标准再次按梯次调高；如此辗转下去，群集的系统解算效应得到充分展现。可以在很短时间内求得全局最优解。根据具体情况，可配置不同的寻优策略，从而进一步加快解算进程。

### 2.2 高适应性核心算法——人工生命算法

对于模型解算的复杂性和时序性难题，单纯依靠硬件和策略均不能有效解决，必须从算法这个根本上寻求突破点，目前最理想的是人工生命算法。

人工生命算法是模拟生物界适应环境、竞争图存和学习进化机制的仿生算法。广义的人工生命算法包括多种遗传算法、蚁群算法和神经网络和部分专家系统系列方法。目前，研究最活跃、应用最广泛、效果最明显的算法首推遗传算法系列，如智能变参遗传算法。采用遗传算法，可以很方便地解决兵力分配、目标选择、战术对策选择等经典难题。对于大型作战方案，它也胜任为核心算法。其基本的寻优原理是，系统首先生成一组方案，然后逐个进行评价，引用轮盘赌等选择机制，以较大的概率选择较好的方案作为基础生成下一代方案，并通过一种称为变异的机制来形成全新的方案。这就保证了对要求的适应性越来越强，方案越来越优。此类算法具备学习和适应性变异能力，通过交流机制取长补短，通过变异机制适应各种限制条件。对作战方案而言，就是新的、更符合优化标准的方案不断生成，从而完成优化。人工生命算法对模型形式和复杂性的适应性极强，只要有衡量标准就能使用，对模型的形式并不敏感，同样适用于求解随机规划、模糊规划等特殊形态模型。

### 2.3 谋略与软件的桥梁——规则引导机制

对方案制定而言，人脑对部分内容有更好的洞

察力，可以直接完成判断，而计算机则需较长时间的搜索。此时可运用规则进行干预引导，将思想和谋略具体化为规则，量化为解算参数，引导搜索方向，加快向最优解的逼近速度。例如：根据系统对抗原理和扬长击短、非对称作战等谋略原则，可直接指定使用远程空对地导弹对敌地对空导弹的制导雷达实施第一波打击；强制指定对某类目标的突击比例不低于 80%；选择某目标为必须打击目标，直接指定突击某目标的所用机型和弹型；优先选用某种机型突击某类目标；从代价及系统效应出发，调整对某类目标的突击效果指标。实践证明，加入的约束越多，搜索空间就越小，寻优过程也就越快。实践证明，规则引导是提高解算效率最灵活也最有潜力的手段。

## 2.4 局部直接优化途径——通用解算组件

如果对模型进行更细致的考察，我们可以发现，大型作战方案中的部分内容可以分解出来，单独进行解算。对于此类局部优化问题，可以引入通用解算组件进行求解。主流解算组件均有相应的解算控制环境，可以在规范的工作界面中直接定制目标函数和约束条件，也可使用 VC 等编程语言调用解算部件，将数据和形式化后的模型传递给它，从而间接完成解算。

目前，较有代表性的通用解算组件有 Solver、Maple 及 Lingo 等。总体上说，Solver 部署方便，较适用于解决战术级的非线性整数规划问题，如中小规模防空作战兵力分配问题等；Lingo 具有完整的编程接口，解算速度优势明显；Maple 则具有符号运算等特殊功能，并在 Matlab 中提供功能覆盖面极其广泛的工具箱。

对于分解后的小规模的非线性整数规划问题，若依靠直接编程来实现求解，核心代码达上万行，且效果一般，但是使用上述通用解算工具，以二次开发形式实现，核心代码仅 50 行左右，可见，这种解决手段有其独特的优势。

## 2.5 推演验证手段——HLA和可视化仿真技术

对大型作战方案而言，验证完善是非常有必要的，具体技术手段如下。

基于 HLA（高层体系结构）的总体作战进程模拟。可以按照总体作战目标、具体作战进程和波

次在时间线上安排模拟的兵力，演示各种作战行动，加入多类随机因素，检验方案的弹性和科学性、可行性，发现问题及时进行调整完善。目前，美军已利用 HLA 和网格体系架构，实现了超过十万个节点的大规模模拟推演。

基于虚拟现实技术的局部作战行动模拟。对于具体的作战行动，还可以采用可视化的虚拟现实技术进行模拟，迅速发现方案数据乃至模型和规则上的具体问题，进而作出调整和修改。对在复杂电磁环境和火力环境中发现和突击目标的情况，各类交战情况，甚至弹药的穿透和爆破情况，都可以进行高分辨率仿真。

## 3 综合解算体系

要全面克服解算难点，获得最高的解算效率，必须构建综合解算体系，集成网格和群集技术、人工生命算法、规则引导机制、通用解算组件和推演仿真等前沿和非常规方法。

### 3.1 综合解算体系架构

综合解算体系集成各种解算途径。人工生命算法实现为核心解算组件，部署在网格主机上；各网格主机通过群集技术整合，并将解算功能调用接口向解算服务注册中心注册；解算服务注册中心存放服务目录；通用解算组件和模拟推演软件配置在解算控制节点。

### 3.2 系统工作模式与流程

解算控制节点确定兵力等资源限制作为约束条件，输入作战意图作为目标函数。可分解出的部分解算任务由本机的通用解算组件直接完成。

解算控制节点通过解算服务注册中心定位网格解算接口，将目标函数和约束条件传给网格主机。

网格主机启动解算服务，在群集中运用算法并执行寻优策略，将中间数据回送解算控制节点。

解算控制节点通过控制界面和规则引导组件引导控制解算进程。

方案产生后，可使用模拟推演组件进行验证和完善。

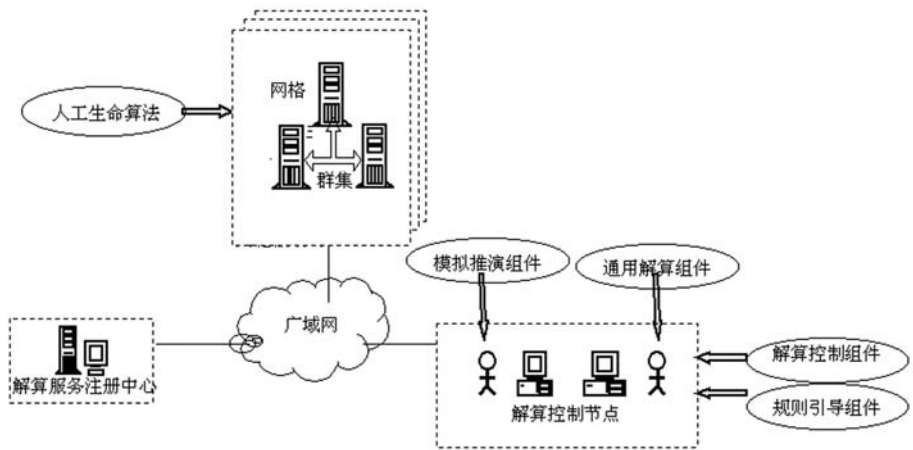


图 1 大型作战方案综合解算体系架构示意图

3.3 综合解算效能分析

大型网格主机：可以有多达 1024 个 CPU，速度可提高约 3 个数量级。

集群解算技术：可灵活配置解算策略，阶跃式提升解算效率，达 3 个数量级左右。

优化的人工生命算法：突破核心难点，提高解算速度 2 个数量级左右。

规则引导机制：提高解算速度 2 个数量级左

右。这方面的潜力很大。

通用解算组件：直接实现局部优化。

推演仿真组件：迅速、逼真地完成方案的验证调整，效率相比实兵验证有大幅度的提升。

综上所述可见，运用综合解算体系，可有效突破大型作战方案的四个解算难点，迅速生成科学的作战方案，支撑实现决策优势。

参考文献

[1] 曾宪钊等.《军事最优化新方法》. 北京：军事科学出版社，2005 年 6 月

[2] 金伟新主编.《大型仿真系统》. 北京：电子工业出版社，2004 年 8 月

[3] 夏靖波等.《网格原理与开发》. 西安：西安电子科技大学出版社，2006 年 4 月

[4] 高尚，杨静宇著.《群智能算法及其应用》. 北京：中国水利电力出版社，2006 年 5 月

作者联系方式

通信地址：空军指挥学院训练部

邮政编码：100097

联系电话：010-66923101 010-66924115

# 指挥控制信息系统防御电磁脉冲武器攻击问题研究

李重一

**摘 要:** 本文综述了电磁脉冲形成原理, 分析了电磁脉冲武器对指挥控制信息系统的毁伤途径和效能, 探讨了指挥控制信息系统防御电磁脉冲武器打击的技术措施。

**关键词:** 电磁脉冲; 指挥控制信息系统; 防护

## 1 引言

核爆电磁脉冲 (HEMP) 和非核爆电磁脉冲 (HPM & UWB), 统称为电磁脉冲弹 (E-Bomb)。作为新型定向能武器, 它对指挥控制信息系统的生存构成了严重威胁。

高强度电磁脉冲对电子设备的破坏作用是美军首先发现的。1963 年 7 月, 美军在约翰斯顿岛进行了一次代号为“海盘车”的高空核试验。这次 140 万吨当量的核爆炸出现了意想不到的情况: 核爆产生的电磁脉冲使远在 1130 公里外的檀香山地区供电、通信系统中断, 甚至导致远在澳大利亚的无线电广播、导航也陷入混乱达 18 小时之久, 但并未造成任何人员损失。这一独特现象引起美国军方高度关注, 并加以研究。鉴于用核爆炸的方法制造电磁脉冲有可能引发核战争, 美军多年来一直试图研发能在常规战争使用的非核爆炸电磁脉冲武器。20 世纪 80 年代后期, 随着相关技术的逐渐成熟, 美军试制了非核电磁脉冲弹, 并随后在海湾战争中试用。据报道, 为干扰、摧毁伊军防空和指控系统, 美海军发射了装有电磁脉冲弹头的“战斧”巡航导弹, 但由于技术欠成熟, 实战效果不佳。美军随即对其进行了改进, 并再次用于实战, 在科索沃、伊拉克战争中取得了预期战果, 高能电磁脉冲武器从此进入了实战化阶段。目前, 电磁脉冲武器已成为实施战略、战术打击的重要武器。

## 2 电磁脉冲的产生及影响

### 2.1 形成原理

电磁脉冲的形成原本是一种自然现象, 雷电、太阳风等均可生成强电磁脉冲。以雷电现象为例:

当空中带电云层大量堆积时, 一旦电场强度超过临界值, 就会击穿空气发生强烈放电, 并在电流路径周围感生高强度电磁脉冲; 核爆炸也能产生高能电磁脉冲, 当爆炸发生时会产生大量 $\gamma$ 射线, 由于康普顿效应 (Compton Effect),  $\gamma$ 射线与空气分子反应后会在爆点周围形成电荷堆积区。此时负电子会沿径向高速外移, 在  $10^{-8}$  秒内形成一个正电荷在内, 负电荷在外的空间电场。由于环境的不均匀性, 电场很难长时间保持均衡对称, 一旦平衡被打破, 电荷堆积区内就会产生强烈的瞬间径向电子束流, 并激发高能电磁脉冲辐射。

### 2.2 电磁脉冲武器

电磁脉冲武器就是依据上述原理制造的强电磁脉冲辐射装置, 它与激光武器、粒子束武器并称三大定向能武器。按电磁脉冲生成方式不同, 可区分为核电磁脉冲弹与非核电磁脉冲弹两类。

#### 2.2.1 核电磁脉冲弹

核电磁脉冲弹就是小型化的核武器, 它利用核爆炸直接产生高强度的电磁脉冲。在高度约 40000 米的大气平流层之上引爆  $10^3$  吨当量的核弹, 可在瞬间释放出能量达  $9 \times 10^{11} \text{ J}$  的 $\gamma$ 射线。 $\gamma$ 射线与空气作用后衍生大量电子 ( $10^{14}/\text{m}^3$  个), 并迅速生成场强达每米  $10^3 \sim 3.4 \times 10^4$  伏特的电磁脉冲, 其辐射强度足以摧毁目标区内任何不设防的指挥控制信息系统。由于此类电磁脉冲功率巨大, 覆盖范围广阔, 不必准确确定目标位置就可实施打击; 高空核爆炸距目标较远, 其热能、机械能和放射性物质不会对人产生直接伤害。

#### 2.2.2 非核爆电磁脉冲弹

非核电磁脉冲弹是依据磁通守恒原理, 利用爆

炸压缩磁通量的方法制造的高功率电磁脉冲武器。其主要构成部件为“磁通压缩发生器”(FCG, Flux Compression Generator)或“磁流体动力学发生器”(MHDG, Magneto-Hydrodynamic Generator)、炸药、电池及电源、同轴电容器组、平衡环和微波天线等。其基本原理是,利用高爆炸药轰击“磁通压缩发生器”,在其定子绕组建立了初始磁场的情况下短路线圈,使回路电感迅速减少,电流骤然增大,瞬间生成能量达数亿至数十亿焦耳的强脉冲电流。用此脉冲电流驱动微波发生器,并通过天线向外辐射,即可产生强电磁脉冲。非电磁脉冲弹功率较小,杀伤范围有限,需使用精确制导工具准确运载至目标空域,才能有效实施打击。如图1所示。

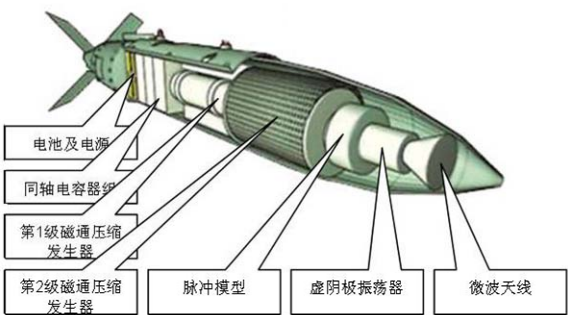


图1 电磁脉冲弹示意图

2.3 电磁脉冲武器的破坏机理及作用

2.3.1 耦合途径

电磁脉冲以电磁波的形式传播耦合到目标,其主要形式主要有以下4种。

天线耦合。雷达、通信系统天线可将电磁脉冲直接引入设备。

电缆耦合。在电磁脉冲作用下,电缆、金属管线会产生感应电流,经传导可耦合至设备。

缝孔耦合。电磁脉冲通过设备金属壳体的缝、孔、窗耦合至设备器件。

介质穿透。电磁脉冲可轻易穿透不设防的建筑物墙壁,也能侵入一定深度的岩土防护层。

2.3.2 破坏机理及作用

电磁脉冲对指挥控制信息系统的影响与雷电相似,但比雷电的作用更强、更广泛。电磁脉冲的破坏能力是通过其特有的强电场效应、强磁场效应、热效应和射频干扰实现的。其破坏作用主要体现在四个方面。

一是干扰。强电磁脉冲本身就是一个宽带射频干扰源,可在信息系统中产生强噪声。电磁脉冲能影响电离层稳定,可使电磁波传播途径发生弯曲。一般而言,当功率密度达  $0.01\sim 1\mu\text{W}/\text{cm}^2$  时,就可造成信号失真、中断。

二是损坏。指挥控制信息系统由大量半导体器件组成,其特性决定了它们耐受强电压、电流冲击的能力很低,当电磁脉冲功率密度达  $0.01\sim 1\text{W}/\text{cm}^2$  时,强电场效应生成的高压就可在半导体电路内部造成击穿现象,从而损坏器件。

三是失效。当电磁脉冲功率密度达  $10\sim 10^2\text{W}/\text{cm}^2$  时,就能在设备壳体上产生瞬态感生电流,耦合进入电磁存储设备(磁心、磁带、硬盘、内存和闪存等)和数字电路后,会因电磁扰动而使记录发生失真、消磁及误码,造成数据失效。

四是摧毁。当电磁脉冲功率密度达  $10^3\sim 10^4\text{W}/\text{cm}^2$  时,强场作用将引发非线性效应,可在电路中引发过热等反应,立即摧毁整个系统。

2.4 破坏范围

2.4.1 空间范围

电磁脉冲弹产生效应的地面区域半径可由下式导出:

$$R = (R_e + H) \cos \left[ \sin^{-1} \left( \frac{R_e}{R_e + H} \right) \right]$$

式中  $R$  为辐射半径,  $H$  为爆炸高度,  $R_e$  为地球半径。由此可得出爆炸高度与影响半径的对应关系如表1所示。

表1 爆炸高度与影响半径的对应关系

爆炸高度(km)	0.5	1	2	5	10	20	40	60	80	100	200	400
影响半径(km)	80	113	160	252	357	505	715	876	1013	1133	1609	2293

2.4.2 频谱及强度

时域下的电磁脉冲场强可用双指数函数表示：  
 $E(t) = E_0(e^{-\alpha t} - e^{-\beta t})$   
其中： $E_0 = 5.25 \times 10^4 \text{V/m}$ ， $\alpha = 4 \times 10^6 \text{ s}^{-1}$ ， $\beta = 4.76 \times 10^8 \text{ s}^{-1}$

上式经傅立叶变换可转换到频域下：

$$E(\omega) = E_0 \left( \frac{1}{j\omega + \alpha} - \frac{1}{j\omega + \beta} \right)$$

电磁脉冲产生的能量可以用下式表示：  
 $W = \int P dt = \int (E^2/377) dt$   
其中：W 为能量密度，P 为功率密度。

表 2 电磁脉冲频谱覆盖范围及强度

类别	非核电磁脉冲		核电磁脉冲（HEMP）
	高功率微波（HPM）	超宽带（UWB）	
天线处峰值功率	100 MW ~ 20 GW	几 GW ~ 20GW	50000TW
脉冲半高宽	< 10ns ~ 1μs	< 10ns	< 20ns
上升时间	10 ~ 20ns	< 1ns	1 ~ 5ns
脉冲输出能量	100J ~ 20kJ	5J ~ 500J	10 <sup>6</sup> GJ
覆盖频带	500MHz ~ 10GHz	100MHz ~ 50GHz	0 ~ 200MHz
初始能量密度	20kV/m ~ 300kV/m	4kV/m ~ 20kV/m	50kV/m

3 指挥控制信息系统对电磁脉冲的防护

指挥控制信息系统防御电磁脉冲武器攻击的基本方法，就是针对脉冲侵入耦合途径及破坏机理，封堵电磁脉冲侵入路径，将有害电磁场屏蔽在系统之外。

3.1 环境防护

环境级防护是对指挥信息信息系统的开设场所进行防护。其主要作法是用导电、导磁材料对坑道、地面建筑、海上舰船等指挥部位进行整体屏蔽，使电磁场能量穿过屏蔽体时因反射和吸收受到严重衰减，从而达到将电磁脉冲阻挡隔绝在信息系统设置空间之外的目的。

3.1.1 坑道设施防护

测试数据表明，电磁脉冲难以直接穿透有较厚岩土被复的指挥坑道，侵入指控信息系统的主要途径是坑道的出入口、通风口和供电、通信电缆和设备天线入口等，这些部位必须进行电磁脉冲防护加固。为解决坑道口部的屏蔽问题，应设置笼型金属网罩住坑道口，并用金属材料制造坑道防护门，网、门应有一体化的良好接地，从而在坑道口部形成一道能有效阻隔电磁脉冲的“防护墙”；为解决管线等孔口部的屏蔽问题，应采用管线隔离技术、孔

口隔离技术加以防护。对暴露的孔口采用金属隔板多层封堵，对通过口部的金属管线及电缆金属护套应与隔板一体接地，从而在管线孔口部形成一个能有效阻隔电磁脉冲的“保护盖”。

3.1.2 地面设施防护

为防止电磁脉冲进入开设指控信息系统的地面建筑物，必须对墙壁、门窗和电缆入口进行防护。墙壁处理的方法主要有三种。一是墙体加厚。增加墙壁厚度是对抗电磁脉冲简单经济的方法。据测试，混凝土厚度每增加 10mm，就可对 450MHz~1500MHz 频段的电磁冲产生 2.5~5db 的反射、吸收衰耗；二是使用抗电磁辐射墙布、涂料。据测试，在墙壁上粘贴不同厚度的金属聚酯纤维织物，可对 0.3~180MHz r 的电场可产生 20~80db 衰减。也可在墙壁上喷涂含金属成份的涂料，此方法的效能与金属聚酯纤维织物类似。三是在墙壁内部加衬高密度金属网或 0.5mm 以上厚度的金属板，此法可对电磁脉冲生成的电场、磁场产生 40~100db 的衰减；门窗及孔口的屏蔽处理方法。一是采用导电导磁良好的金属材料制作门窗，并做良好接地。为使门窗面板与框接触良好，门窗与框的结合部位应使用导电导磁密封件连结。二是采用金属网整体封闭窗体，并辅之以金属纤维质窗帘，防止电磁脉冲由缝隙侵入。三是孔口屏蔽。采用与坑道孔口防护相同的措施封堵管线、电缆入口。需要特别注意的是，建筑物各立面（墙、顶板、地板）及

门、窗和孔口宜采用相同材质的防护材料,可提高屏蔽的整体性。

### 3.1.3 野战及舰载设施防护

鉴于金属材料制成的密闭仓室对电磁脉冲有良好的质的反射、吸收作用,因此,野战机动式指控信息系统应置于密闭方仓内,尽可能避免在置于帐篷内和暴露于野外。舰载指控系统应尽量置于水线之下无舷窗的密闭仓室。方仓及舰艇指挥仓门窗、电缆引入口应作孔口屏蔽处理,外壳应做良好接地,外接电源、通信天线应加装过压、过流保护。

## 3.2 系统防护

系统级防护是对指控信息系统本身的防护,其重点是对系统的引入天线、机壳等进行屏蔽、隔离和能量释放。一是前端泄放。所谓前端是指系统天线及金属引入线缆,此处是电磁脉冲侵入系统的重要路径。此部位的防护可借鉴以往明线、同轴电缆载波电路防雷电措施,在引入端口加装辉光放电管、火花隙放电器及氧化锌变阻器。放电器非导通状态下要做到基本不损耗系统工作信号,当耦合进入的电磁脉冲电压超过临界值时,放电间隙击穿,把电磁脉冲能量瞬间短路泄放入地,达到保护设备

的目的。二是电源隔离。为防止从电源线缆引入的电磁脉冲烧毁电源,应在电源引入端也使用放电器、氧化锌变阻器,同时加装电源低通滤波设备,削平浪涌电压,隔绝强电磁脉冲对电源输入端的冲击。三是壳体接地。在设置系统的电源地、工作地的基础上设置防电磁保护地,并尽可能降低接地电阻,缩短接地引接体,使机壳、机架、线缆屏蔽层和系统本身接地良好,能将感应电压顺利导入大地。

## 3.3 器件防护

器件级防护是系统最内层的防护,其重点一是要在指挥控制信息系统上尽量采用能耐受强磁强电场的核加固器件,强化器件本身抗强磁强电场的能力。二是在指挥控制信息系统线路设计上要与民用产品相区别,增加强电磁脉冲感应电路和自适应开关、滤波电路,阻止电磁脉冲侵入,提高电路器件抗电磁脉冲武器攻击的防护性能。三是采用光传输技术,尽量减少金属线缆、电路、器件的使用,减少电磁耦合途径;四是加强抗强电磁脉冲器件的研制,解决抗强电磁脉冲加固器件种类不足的问题。

## 参考文献

- [1] Maa, Baw-ming Protection for military facilities against the effect of an electromagnetic pulse
- [2] Yi-wun Li The Study of EMP Protection and Clamping Components
- [3] 周壁华, 陈彬, 高成. 现代战争面临的高功率电磁环境分析 2002.3 微波学报第 18 卷第 1 期

## 作者联系方式

通信地址: 北京市西三环中路 19 号甲 3 信息办海军后勤部信息化工作办公室  
 邮政编码: 100841  
 联系电话: 010-66960533

# 基于灰色模糊物元的装备保障效能综合评估方法

周巍 颜宁 马振江 朱晓华

**摘 要:** 从装备保障性、保障系统、保障效能等方面,论述了装备保障信息化的重要作用。运用系统工程理论,构建了装备保障效能评估的参数指标体系和评估模型,提出了基于灰色理论、模糊数学和物元分析的综合评估方法,为装备保障性设计、保障系统的建立和优化以及装备保障管理提供了有效的决策手段。

**关键词:** 灰色理论;模糊数学;物元分析;装备保障;效能评估

## 1 引言

为使武器装备在作战中适用有效,不仅要求其具有先进的战术技术性能,而且必须具有良好的使用性能,即具有高的可靠性、良好的维修性和高效的保障性,这也正是在武器系统论证采办、研制生产、使用管理和作战运用过程中所必须解决的问题。装备保障作为保持和恢复装备的良好技术状态、改善装备性能的有效措施,直接关系到武器系统的战备完好率和使用效能,已成为武器装备建设链条中的关键环节,成为影响武器系统的寿命周期费用和部队战斗力的一个重要因素。

以信息技术为核心的高新技术的迅猛发展及其在军事领域的广泛应用,促使现代战争呈现出高精度、高消耗、高速度和全方位的高技术特征,特别是近几场局部战争表明,现代战争已由机械化向信息化方向转变,信息技术覆盖了战争的各个方面,信息化战争将成为未来战争的主要作战样式。装备保障体系正是集保障体制、保障资源(包括保障设备、设施、人员、物资器材、技术资料等)、保障管理各种信息为一体的综合信息系统,如何在信息化战争条件下,针对装备实际,考核和验证各项性能指标(包括装备保障性、保障系统、保障效能等)是否满足部队使用和作战需求;如何针对装备的实际使用状况,实施高效的装备保障;如何以未来战备需求为牵引,合理选择装备保障方案,建立与未来战争相适应的装备保障系统;如何统筹考虑各个阶段的工作,综合权衡各项指标,进行装备保障资源的规划建设;如何组织实施装备保障,本着便于平时日常装备技术保障、战时野战抢修的原则,合理优化现行结构,达到精干、合成、高效的

目的,等等,这一系列问题,都要求进行深入的研究和系统的分析。然而,装备保障是一项复杂的系统工程,仅靠传统的方法只能够局限在单一指标评估和静态分析的基础上,难以对装备的使用性能进行系统的分析和评估,不能对装备保障的合理性和保障的整体效能进行综合权衡,从而也就难以及时反馈装备使用性能和装备保障的具体信息,难以正确选择和优化装备保障形式、内容和规模。因此,从装备和部队使用实际出发,充分利用现代信息技术和手段,建立相应的参数指标体系和评估模型,对装备保障效能进行综合评估,已成为亟待解决的重要课题。

装备保障效能评估和资源优化是装备信息化的重要内容之一,也是在论证采办、研制生产、使用管理和作战运用过程中所必须解决的重要问题。其目的是验证装备的保障性、保障方式是否满足装备使用和作战需求,评估装备保障的适应程度,以保证装备达到规定的可用性要求,提高装备保障的整体效能。虽然装备在立项论证过程中,曾提出了装备保障性要求,在设计过程中,也曾制定了装备保障性设计准则,规划了装备保障系统,但这些措施并不能验证产品是否满足所规定的使用和装备保障要求,也不能对装备保障能力做出准确估计与评价。这就难以对武器系统实施科学的装备保障,装备保障系统也就不可能协调有序的运行。因此,还必须在信息化战争条件下对装备保障指标体系进行综合评估,将得到的相关数据资料用于装备保障能力的分析与评定,并在此基础上,改进装备保障方式、方法和手段,提高装备的装备保障效能。

由于武器系统的复杂性以及装备保障效能指标的不明确性和不相容性,很难对其进行准确评估。



本文针对信息化战争条件下装备保障的特点，运用系统工程理论，构建了装备保障评估的参数指标体系和模型，提出了基于灰色理论、模糊数学和物元分析的装备保障效能综合评估方法，以期为保障性设计、保障系统的建立、保障资源的优化配置和管理以及战时保障部署和指挥提供科学决策的依据和手段。

2 装备保障效能评估指标体系

评价指标体系是一个从多视角、多层次反应特定客体的信息系统，能否合理地确定评价目的、评价指标和评价策略是做好装备保障效能评估的关

键。即使是同一评价对象亦可以有不同的评价目的，从而导致不同的评价标准和评价方法。武器装备保障评价总的目标是评估系统的装备保障性是否满足使用需求，评估装备保障系统的功能，以便不断地修改完善，保证其与主战装备匹配、有效而经济地运行；评估系统的装备保障效能，降低装备的寿命周期费用，提高效费比。

装备保障评价工作的目的性主要由评价指标体现。由于装备保障涉及多种属性，所以，为了反映评价目的，需要明确评价目标体系。评价目标体系是评价指标体系的核心和纽带，图 1 给出了装备保障评价目标体系。对不同的装备，其目标会略有差别。

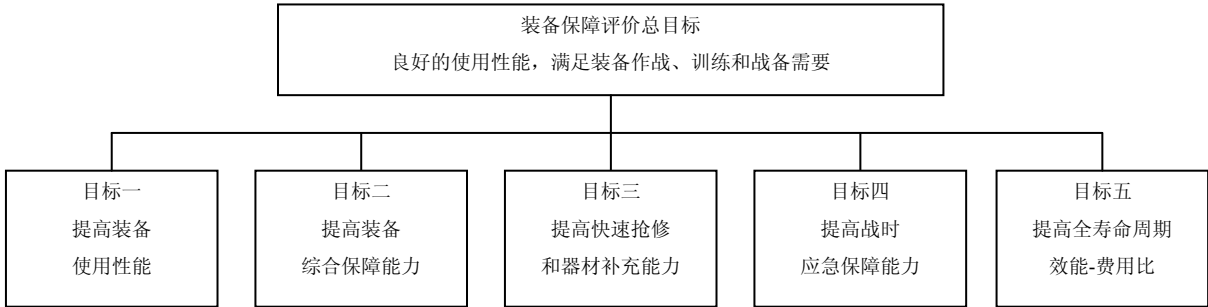


图 1 装备保障评价目标体系示意图

评价指标是目标的具体反映。装备保障综合评估指标体系的确定应遵循系统性、准确性、实用性的原则。通常，装备保障评估指标有多种设计模式，根据装备使用和作战需求，采用如图 2 所示的指标体系。

装备保障效能评估指标体系分四大类用  $C=(C_1,C_2,\cdots,C_n)$  表示， $n=4$ ，每一类  $C_i$  有  $m$  个评价因子，即  $C_i=C_{i1},C_{i2},\cdots,C_{im}$ ，其中  $C_{ij}$  表示第  $i$  类中第  $j$  个评价因子。

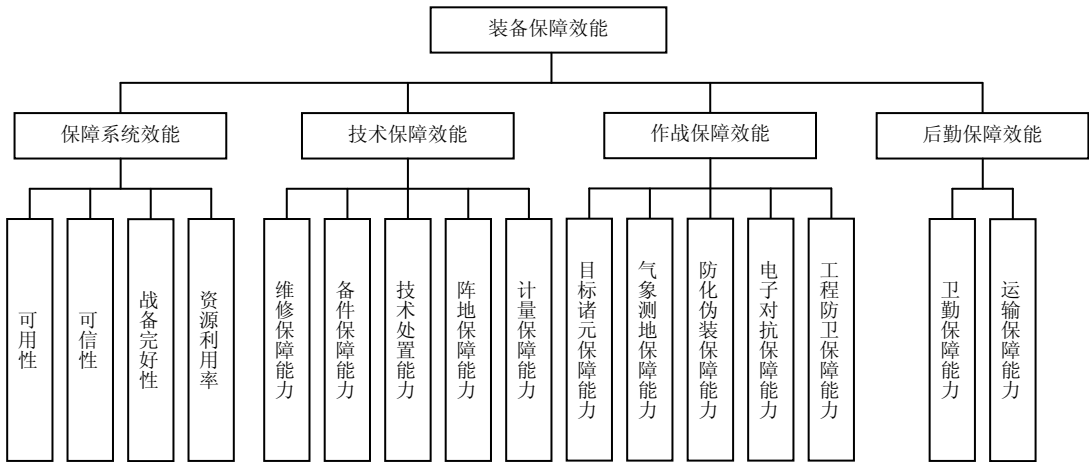


图 2 装备保障效能评估指标体系

3 装备保障效能评估模型

3.1 系统建模

系统模型的建立是一个反复修改、不断完善的过程，应依据装备和使用实际，建立与实际装备相匹配的评估模型。本文根据装备保障效能评估需求，将灰色理论、模糊数学和物元分析方法相结合，构建了装备保障效能综合评估模型，并用层次分析法确定了权重系数。系统的建模步骤如图 3 所示。

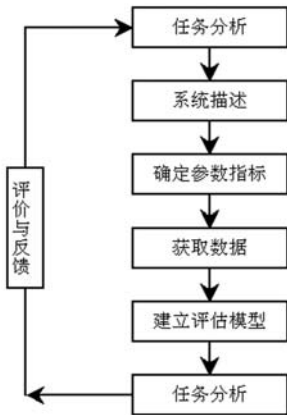


图 3 综合评估模型的建立流程

3.2 模糊物元和复合模糊物元

给定事物的名称  $M$ ，它关于特征  $c$  的量值为  $u$ ，以有序三元组  $R = (M, c, u)$  作为描述事物的基本元，简称物元。若其中的量值具有模糊性，则称为模糊物元。记做：

$$R = \begin{bmatrix} M \\ c \quad u(x) \end{bmatrix} \tag{1}$$

其中： $M$  为事物的名称， $c$  为  $M$  特征， $u(x)$  为与特征  $c$  相应量值  $x$  的隶属度。若事物  $M$  有  $n$  个特征  $c_1, c_2, \dots, c_n$ ，与其相应的模糊量值为  $u(x_1), u(x_2), \dots, u(x_n)$ ，则称  $R$  为  $n$  维模糊物元。若以  $R_n^m$  表示  $m$  个评价样本的  $n$  维复合模糊物元，并以  $M^e$  表示第  $e$  个评价样本， $C_i$  表示第  $i$  项评价指标，与其相应的模糊量值为  $u_i^e(x_i)$  ( $i=1,2,\dots,n; e=1,2,\dots,m$ ) 则有：

$$R_n^m = \begin{bmatrix} M^1 & M^2 & \dots & M^m \\ C_1 & u_1^1(x_1) & u_1^2(x_1) & \dots & u_1^m(x_1) \\ C_2 & u_2^1(x_2) & u_2^2(x_2) & \dots & u_2^m(x_2) \\ \dots & \dots & \dots & \dots & \dots \\ C_n & u_n^1(x_n) & u_n^2(x_n) & \dots & u_n^m(x_n) \end{bmatrix} \tag{2}$$

3.3 模糊物元的隶属度

本模型基于灰色理论与模糊物元，即用灰数白化值来表示事物的量值，其隶属度用灰类和白化函数来计算。在武器系统指标的评价中，将指标的等级划分为“优”、“良”、“中”和“差”四个级别，其等级评分标准如表 1 所示。将各等级看作事物，将各指标作为特征。设有  $k=1, 2, \dots, p$  个专家分别对评估指标  $C_{ij}$  按表 1 的等级标准进行评分，第  $k$  个专家对指标  $C_{ij}$  的评分用  $d_{ijk}$  表示。

表 1 指标等级划分表

等级	优	良	中	差
指标分值	$8 \leq d < 10$	$6 \leq d < 8$	$4 \leq d < 6$	$0 \leq d < 4$

3.3.1 确定评价灰类

评价灰类的等级数、灰数以及白化权函数的确定与具体对象和等级的划分有着重大关系，根据本文具体情况，采用如下白化权函数：

第一类“优”类，灰数  $\otimes_1 \in [0, 8, +\infty)$ ，白化权函数为：

$$f_1 = \begin{cases} d_{ijk}/8 & 0 < d_{ijk} \leq 8 \\ 1 & 9 \leq d_{ijk} \\ 0 & \text{其他} \end{cases} \tag{3}$$

第二类“良”类，灰数  $\otimes_2 \in [0, 8, 16]$ ，白化权函数为：

$$f_2 = \begin{cases} d_{ijk}/8 & 0 < d_{ijk} \leq 8 \\ 2 - d_{ijk}/8 & 8 \leq d_{ijk} \leq 16 \\ 0 & \text{其他} \end{cases} \tag{4}$$

第三类“中”类，灰数  $\otimes_3 \in [0, 4, 8]$ ，白化权函数为：

$$f_3 = \begin{cases} d_{ijk}/4 & 0 < d_{ijk} \leq 4 \\ 2 - d_{ijk}/4 & 4 \leq d_{ijk} \leq 8 \\ 0 & \text{其他} \end{cases} \tag{5}$$

第四类“差”类，灰数  $\otimes_4 \in [0, 2, 4]$ ，白化权函数为：

$$f_4 = \begin{cases} 1 & 0 < d_{ijk} \leq 2 \\ 2 - d_{ijk} / 2 & 2 \leq d_{ijk} \leq 4 \\ 0 & \text{其他} \end{cases} \quad (6)$$

### 3.3.2 确定隶属度

对评价指标  $C_{ij}$ ，第  $e$  个评价灰类的隶属度记为  $u_{ij}^e$ ，令：

$$u_{ij}^e = \frac{\sum_{k=1}^p f_e(d_{ijk})}{\sum_{e=1}^g \sum_{k=1}^p f_e(d_{ijk})} \quad (7)$$

## 3.4 计算权重系数

利用层次分析法确定权重系数，其主要步骤如下。

① 建立层次结构模型。在深入分析问题的基础上，将有关因素按照不同属性自上而下分解成若干层；② 构造判断矩阵。将同一层次因素一定的准则下两两比较其相对重要程度，并用一定的标度量化方法建立判断矩阵；③ 计算相对权重向量；④ 进行一致性检验。对得到的权重系数是否满足要求要对判断矩阵进行一致性检验，来验证权重系数的合理性。

## 3.5 欧氏贴近度和评价

考虑到本文的综合评价意义，采用  $M(\bullet, +)$  算法，即先乘后加运算欧氏贴近度  $\rho H$ ，则指标  $C_i$  的欧氏贴近度为：

$$\rho H_i^e = 1 - \sqrt{\sum_{j=1}^n w_j (u_{ij}^e - u_{ij}^0)^2} \quad (8)$$

其中， $R_n^0 = \begin{bmatrix} C_{i1} & C_{i2} & \cdots & C_{in} \\ M^0 & u_{i1}^0 & u_{i2}^0 & \cdots & u_{in}^0 \end{bmatrix}$  为理想物元，

理想物元的选取可按相对优化原则，选定各项指标相应的灰数白化值中最大值、最小值或适中值，以构成新物元，根据具体情况这里取理想物元为  $R_n^0 = \begin{bmatrix} C_{i1} & C_{i2} & \cdots & C_{in} \\ M^0 & 1 & 1 & \cdots & 1 \end{bmatrix}$ ； $w_j$  为第  $j$  个指标的权重系数。 $\rho H_i^e$  表示第  $e$  个物元与理想物元的相近程度，其值越大，表示两者越接近；反之，则相差越大。

## 3.6 系统效能评估的综合评价

由式 (8) 得到指标  $C_i$  的欧氏贴近度  $\rho H_i^e$ ，令：

$$\rho H_{\text{总}}^e = \sum_{i=1}^t w_i \rho H_i^e \quad (9)$$

其中， $t$  为一级指标的个数。由  $\rho H_{\text{总}}^e$  的大小的意义对其进行等级的评定。

# 4 评估系统设计

## 4.1 系统构成

根据装备保障评估任务需求分析，装备保障评估系统的组成如图 4 所示。

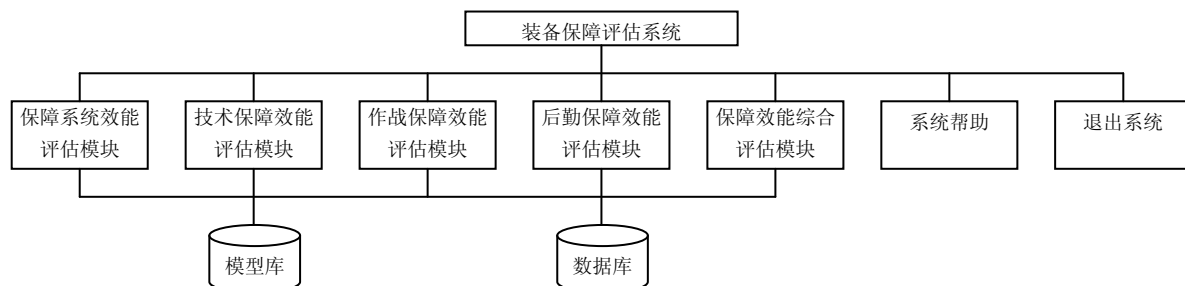


图4 装备保障综合评估系统组成结构图

## 4.2 评估流程

装备保障综合评估系统的功能流程如图 5 所示。

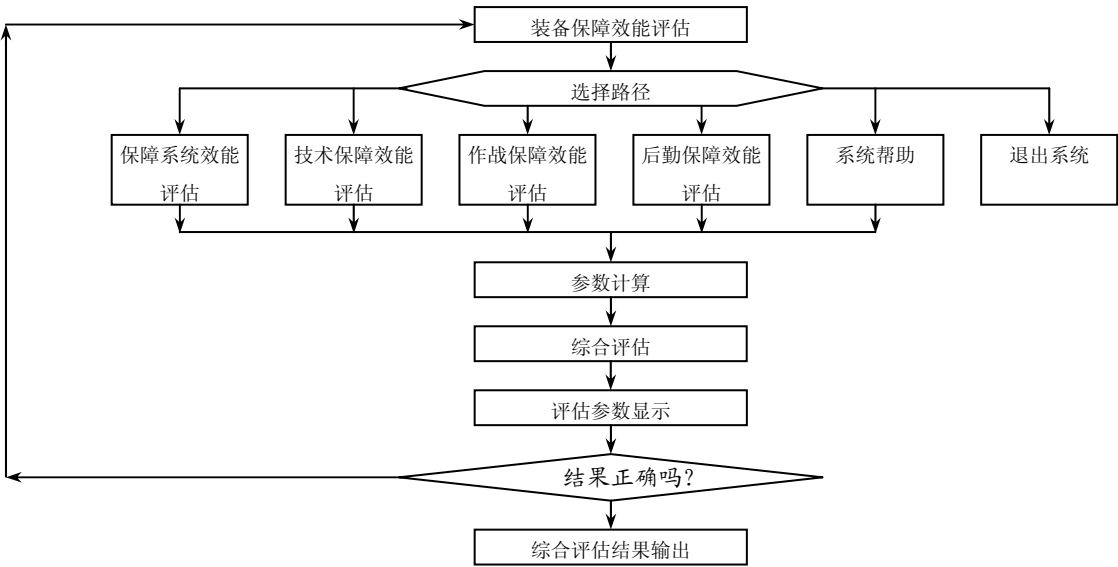


图 5 装备保障综合评估系统功能流程图

5 应用实例

各个指标按表 1 的评分等级标准进行打分，用层次分析法原理计算各个指标的权重系数，结果如表 2 所示。

假设选取 5 位专家对某型武器装备保障系统的

表 2 指标权重及评分表

	指标		权重系数		专家				
			w	w <sub>i</sub>	1	2	3	4	5
	保障系统效能	可用性	0.3373	0.3911	8	8	7	9	8
可信性		0.3209		9	7	8	9	7	
战备完好率		0.1578		7	6	7	6	6	
资源利用率		0.1402		7	9	8	7	6	
技术保障效能	维修保障能力	0.2198	0.3649	9	9	8	9	7	
	备件保障能力		0.3603	8	9	8	7	9	
	技术处置能力		0.1114	8	7	9	8	7	
	阵地保障能力		0.0919	9	9	8	7	9	
	计量保障能力		0.0716	7	7	6	7	7	
作战保障效能	目标诸元保障能力	0.3167	0.6105	9	8	9	8	9	
	气象测地保障能力		0.5607	8	9	8	9	8	
	防化伪装保障能力		0.5113	8	9	9	8	8	
	电子对抗保障能力		0.5071	8	8	8	9	9	
	工程防卫保障能力		0.4393	9	8	7	9	8	
后勤保障效能	卫勤保障能力	0.1262	0.3537	8	7	8	7	8	
	运输保障能力		0.1568	8	6	7	7	7	

以“保障系统效能”为例，由公式（3）～（7）可得其模糊物元矩阵为：

$$R_{\text{保障系统}} = \begin{bmatrix} & M^0 & M^2 & M^3 & M^4 \\ C_{11} & 0.4937 & 0.4810 & 0.0253 & 0 \\ C_{12} & 0.4872 & 0.4615 & 0.0513 & 0 \\ C_{13} & 0.4000 & 0.4000 & 0.2000 & 0 \\ C_{14} & 0.4186 & 0.4070 & 0.1744 & 0 \end{bmatrix}$$

由公式（8）得“保障系统效能”的欧氏贴近度为：

$$\rho H_{\text{保障系统}} = (0.4626, 0.4482, 0.0743, 0)$$

同理可得：

$$\rho H_{\text{技术保障}} = (0.4950, 0.4686, 0.0363, 0)$$

$$\rho H_{\text{作战保障}} = (0.5071, 0.4815, 0.0112, 0)$$

$$\rho H_{\text{后勤保障}} = (0.4378, 0.4378, 0.1211, 0)$$

由公式（9）得：

$$\rho H_{\text{总}} = (0.4807, 0.4619, 0.0519, 0)$$

根据贴近度的含义，该导弹武器系统的保障效能属于“优”层次。

## 6 结束语

本文运用系统工程方法，通过对武器系统的分析，建立了装备保障效能评估指标体系，将灰色理论、模糊数学和物元分析方法有机结合，构造了适合于装备保障效能评估的模糊物元模型，提出了一种装备保障效能综合评估的新方法，实现了对武器装备保障效能优劣程度的评价。并利用层次分析法确定了各个指标的权重系数，最后通过实例对此模型进行了验证。结果表明，模糊物元以解决不相容问题为核心，适用于多因子评价问题。该方法可对装备保障效能进行有效的评估，为装备保障规划、进行保障部署、定下保障决心和筹划保障行动提供科学的依据和支持。

## 参考文献

- [1] 李廷杰. 导弹武器系统的效能及其分析[M]. 北京：国防工业出版社，2000.
- [2] 陈学楚. 装备系统工程[M]. 北京：国防工业出版社，1995.
- [3] 甄涛，王平均，张新民. 地地导弹武器作战效能评估方法[M]. 北京：国防工业出版社，2005.
- [4] 张斌，雍歧东，肖芳淳. 模糊物元分析[M]. 北京：石油工业出版社，1997.
- [5] 赵焕臣. 层次分析法[M]. 北京：科学出版社，1986.

## 作者联系方式

通讯地址：北京市海淀区清河大楼子八

邮政编码：100085

联系电话：010-66345310

# 数据链与相对时空参照系

徐恩秀

**摘要：**从军事功用的角度，阐述了数据链的主要作用是建立时空参照系，网内成员相对时空参照系是如何建立的，相对时空参照系的作用和意义。

**关键词：**数据链；时空参照系；相对；网络中心战

数据链是什么？提问的人往往得不到满意的回答。答案之所以不能令人满意，在我看来，主要因为看待数据链这一事物的角度不同。问的人往往站在功效作用的角度，解释的人则经常从技术实现出发。

数据链是因特定需求而产生，又根据需求变化不断演进的一项装备，完全是一个实用主义的产物。单从“数据通信”、“数据+链路”、“数据链路”等技术概念出发去解释、定义或理解数据链，就很难给出让人满意的答案。

在数据链的大量定义中，我喜欢其中一种描述性定义：数据链是集通信、定位、导航、识别等功能为一体的集成装备。

## 1 建立时空参照系是数据链的主要目的

数据链的集成，不是为集成而集成。它集成的目的是要“给信息赋予明确的时间和位置属性”。给信息赋予明确的时间和位置属性的目的，又是为了在信息交互过程中，“顺手”建立网内成员相对时空参照系。由于建立了相对坐标系，各成员所播发的消息，都自动附加了明确的位置坐标和时间坐标。这样网内成员之间就具备了精确协同的条件，网络中心战就有了物质基础。

注意，这里所说的给信息赋予时间和位置属性，是说将信源的时空坐标作为信息的组成部分，这对于信息利用有重要的参考价值。比如：甲发出一条“发现 XX 目标”的消息，同时还附带了“我是在什么时刻，什么位置看到该目标的”，乙收到这条消息时通过推算可以得出相当于自己在某个时刻和位置上所看到的目标，如果推算结果已经超出攻击或防备攻击的时空范围，该条消息就没有实际意义了。这与另外单独交换时间和空间信息在意义

上存在很大不同。

在传统战斗中，作战协同停留在较高的层次，靠人执行协同计划来保证，协同所要求的位置和时间精度相当粗略，协同时效在分钟级以上，协同通信保障无需建立特定的时空参照系，通信双方往往也不太关心对方发信的确切时间和地点，高级别指挥所甚至不希望暴露自己的方位。

在传统的“平台中心战”，确切地说是“基于平台的战斗”中，战斗效能的发挥基于单个武器平台或武器系统。构成指控系统闭环的要素——传感器、控制器、执行器同处一个平台，对于射击而言，相当于自己瞄自己打，这和步枪差不多。间瞄火炮稍微复杂一些，需要以炮兵测地为基准，将前观、雷达、炮阵地、目标纳入一个参照系并控制误差才能保证射击效果，这个参照系往往是以大地为参照并且需要在射击前建立。

但是，将来如果把前观放在直升机上，或由另外一个体系的传感器指示目标，那么它们如何以先前的炮兵测地基准报告目标位置，如何随时加入炮兵群业已建立的参照系呼唤火力指示目标就成为问题。除非大家都用大地参照系，并各自分别满足射击所要求的方向、位置、高程精度。然而保证这个精度的代价很大。但在基于网络的战斗（即网络中心战）中，传感器、控制器、执行器这些指控要素将跨越平台互相作用（如图 1、图 2 所示）。将参加战斗的所有平台都纳入绝对参照系，即均以大地坐标和天文时间为基准，并且保证射击所要求的精度是十分困难的。其实，在一个较大规模的战斗中，协同是分层次的。各个协同层次的时效要求和位置、时间精度要求是有区别的。指挥单元间主要围绕计划的执行与监督开展协同活动，视野较大（通常范围是上一级、下两级），时效要求不高（分钟级即可），协同信息主要是供人使用的文、

图、表。传感器单元、控制单元、武器单元等战斗单元则主要就行动过程展开协同,协同信息主要是时间、位置、距离、状态、目标跟踪标定等数据,且交互对象主要不是人,视野通常集中在战斗组群及对抗空间内。

参与战斗的平台,各有各的任务,它们一定会按行动计划和任务性质分成若干组,高精度的即时协同往往发生在同一组内。数据链所建立的相对时空参照系很轻松地就能满足这种行动分组内的高精度即时协同的需要。

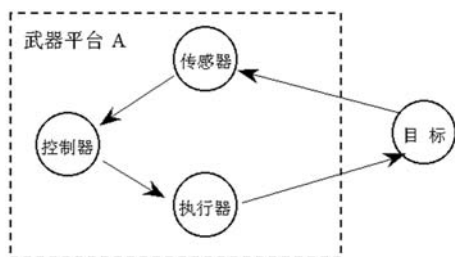


图1 单平台的指控系统闭环

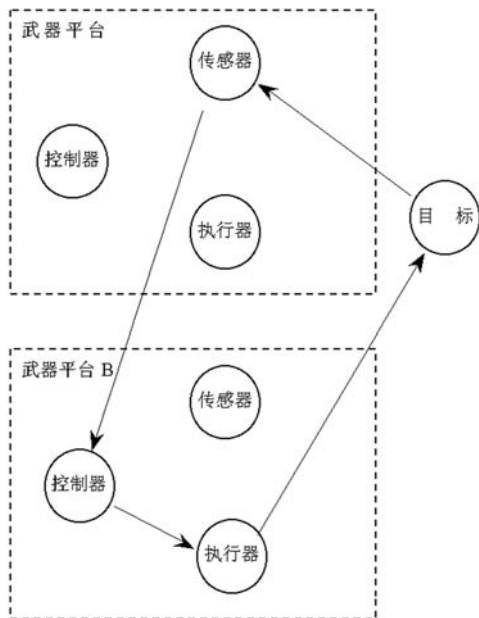


图2 多平台的指控系统闭环

## 2 网内成员相对时空参照系如何建立

对于时分复用的数据链系统,终端入网需要“粗同步”和“精同步”,同步过程通过系统指定一个(且只能有一个)终端为时间基准;基准终端对外广播系统时间和入网报文;欲入网终端捕捉入网报文并发送往返计时报文等一系列动作实现。某个数据链终端一旦实现了精同步,不仅可以开始通

信,而且还和网内成员保持着同一时间基准,往返计时不仅可以测量两两平台间的距离,还精确地给出平台间获得同一信息的时间差,相对时间参照系就此建立。当平台超出视距范围或受到干扰时,终端将回到粗同步,重新进行往返计时,设法重新保持同步。如果该平台偏移系统时间太远,则需要重新入网,回归该参照系。

因战术数据链系统以时分多址同步通信方式工作,每个成员必须不断地与“系统时”较时同步。利用校时过程中测得的消息到达时间实现成员之间精密距离的测量,再加上成员之间位置数据的交换,解算出相互间的距离。这样只要在时分多址同步通信功能的基础上,增加一定的数据处理软件,并与推测导航系统接口就可实现“相对定位和推测导航”功能。相对空间参照系也就此建立。该功能为进入网内的成员提供相互间精确的相对位置数据。当网内成员有两个和两个以上能准确知道自己的地理位置时(如利用GPS定位),便能对该相对坐标系进行地理定位,把该相对坐标系与地理坐标系关联起来。相对定位导航的高准确度,弥补了现行短基线导航和自主式导航定位误差大的缺陷。满足了现代战斗机和精确武器系统对定位的高准确度要求。同样,系统的识别功能也是建立在各成员之间交换位置数据和识别数据的基础上。

## 3 相对时空参照系的作用和意义

数据链就是这样一种以军事需求为牵引,逐渐演变成熟的集成装备。所谓“集成”就是用一种信号格式(波形),一个高频传输通道,一套硬设备,同时完成战术行动所要求的通信、定位、导航和识别功能,而不是简单的设备叠加或功能堆砌。

相对时空参照系的作用和意义远不止上文所述,更大的现实意义在于奠定网络中心战的物质基础。

网络中心战概念基于以下观点:把各种不同的武器系统与传感器连接在一起,将能产生比各个军舰、飞机、潜艇单独使用(即平台中心战)更大的效益。

网络中心战的强大威力来自于高效的网络系统。美军为网络中心战所规划的网络系统由联合规划网、联合数据网、联合合成跟踪网三层网络结构而成。这三层网络所指,均为作战应用网络,不是指物理通信网络。数据链是构建中间层次联合数据网的主要物质基础。

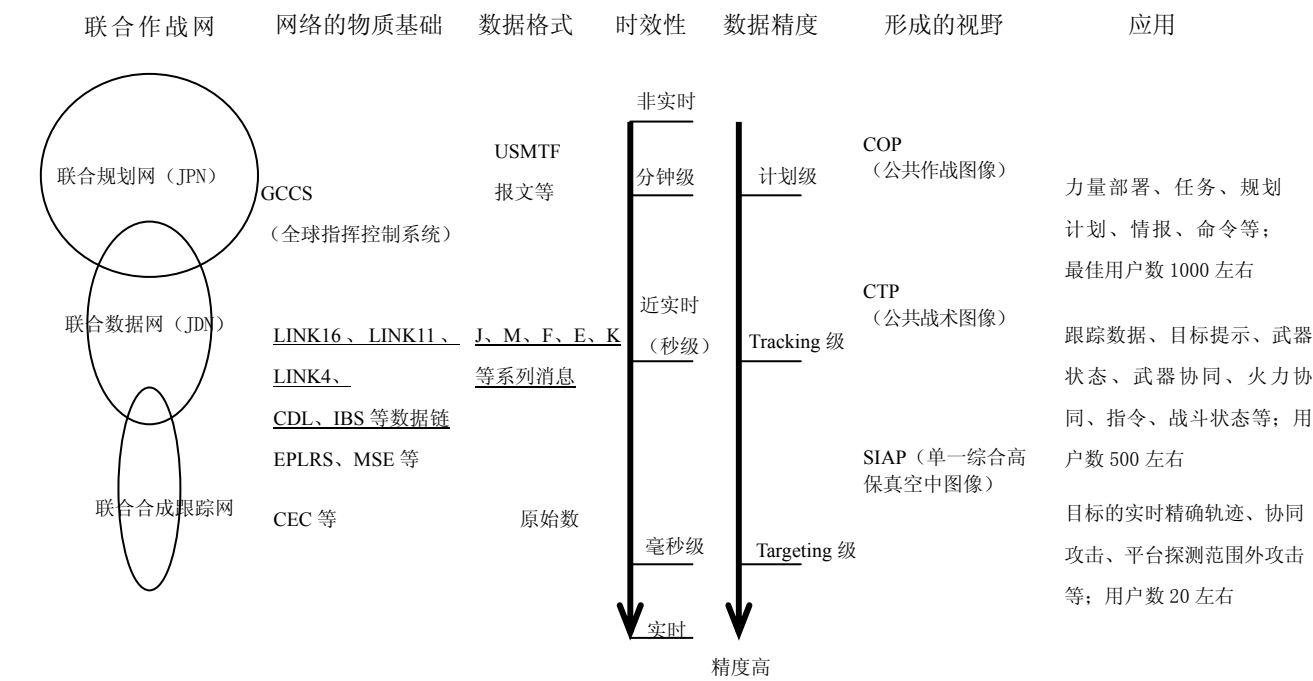


图 3 数据链于网络中心战的地位和作用

数据链所构成的网络与第一层网络相比有一个显著的特点，就是传送的信息是基于比特的格式化消息，这样做一是为了节省带宽，二是因为接收和发送信息的实体主要是应用程序而不是人。另一个特点是采用了一种类似于会议的通信方式，一人说话大家听着，信息有用的就用，没用就当耳旁风，虽说只是听了一耳朵，但在不经意间，网内各个成员的状态、视野就为与会每一个成员所掌握（态势融合以形成公共战术“图像”）。一人发现目标就如同全体都发现这个目标，一个平台能锁定目标就等于该战斗群所有武器平台都锁定了这个目标（共享态势）。这一点对于网络中心战十分重要，它使协同攻击成为可能。

基于这种通信目的，如果所交互的信息没有附带明确的时间和位置属性，你就无法知道小组其他成员是在什么时刻什么位置看到的目标，那么这个目标信息充其量只具有参考意义。但是，当你从另一个平台传感器获得目标信息时，你不仅知道目标自身属性，还知道那个平台是在什么时刻，从什么位置看到的目标，通过时间距离解算，换算成相当于你站立点所看到的目标，再考虑目标的移动方向、速度，武器的末制导和杀伤范围，就可以发射

导弹了。给信息赋予明确的时间和位置属性是数据链通信的第三个特点。上述三个特点的设计目标都是为了将战斗群所有成员的传感器、执行器和目标纳入同一个参照系。

战斗群内有动作协同，战斗群间也有动作协同，无非是协同量较少，但往往十分关键和重要。相对时空参照系之间，通过时间基准和位置基准的交互和换算可以连通。战斗群内如果有一个成员能够获得大地参照系的精确坐标，其他成员亦可纳入大地参照系。从微观上讲数据链的引入可以实现战斗群的协同攻击（群狼战术）；从宏观上讲数据链可以将一线战斗平台的视野扩展至 RC-135 电子信号侦察机、U-2S 侦察机、E-3A/E-2C 预警机、E-8 低速目标和静止目标下视侦察机、EP-3E 水面水下电子信号侦察机乃至“天眼”卫星网的视野。当然这种视野拓展不是单靠某型数据链就能实现的。具有各种不同能力和手段的传感器通过数据链等集成为一个大的侦察网络，用以搜索、跟踪重要目标，并在有关控制器的干预下，标定目标诸元并分配给最适当的执行器。数据链对这种传感器—控制器—执行器广义网络作用贡献很大，也是它的军事价值和意义所在。

参考文献（略）

作者联系方式

通信地址：北京市丰台区大成路 13 号 Z00      邮政编码：100039      联系电话：010-66820166    13601373137



# 运用遗传算法实现多星遥感任务规划

陈健 郭建恩 王鹏

**摘 要：**本文首先对卫星遥感任务的规划现状与特点进行了分析。然后在遗传算法算法分析的基础上，提出了利用多目标遗传算法解决多星遥感任务的规划问题的原理、流程和实现方法。本文在最后讨论了如何根据多星遥感任务规划特点对遗传算法进行优化的方法，并给出了优化的试验比对结果。

**关键词：**卫星；遥感任务规划；遗传算法

## 1 前言

随着我国遥感事业的发展，同时在轨运行并具有不同类型传感器的遥感卫星数量逐渐增多，为了适应未来多星在轨运行业务管理的需求，统筹兼顾利用好这些卫星的遥感器资源，发挥它们的最大综合效益，快速完成卫星遥感计划的制定，需要进行多卫星、多传感器和多地面站条件下的卫星遥感任务智能规划。目前国内还没有针对多星遥感任务进行规划的系统，卫星任务规划需要操作人员根据用户需求及卫星的各种约束条件人工分析，一旦出现问题，则需重新全部分析。这种方式不利于从整体

上协调航天遥感系统的遥感资源和接收资源。

## 2 问题的提出

由于多星的遥感任务规划是根据各自的遥感任务和运行状况来安排计划，其遥感计划只是实现了各卫星的局部优化，只能获得一种可行但非最优的拍摄计划，资源利用率较低，没有实现整个遥感资源的统筹安排和优化。可见，多星遥感任务规划问题是一种典型的多目标优化问题。图 1 给出了问题示意图。

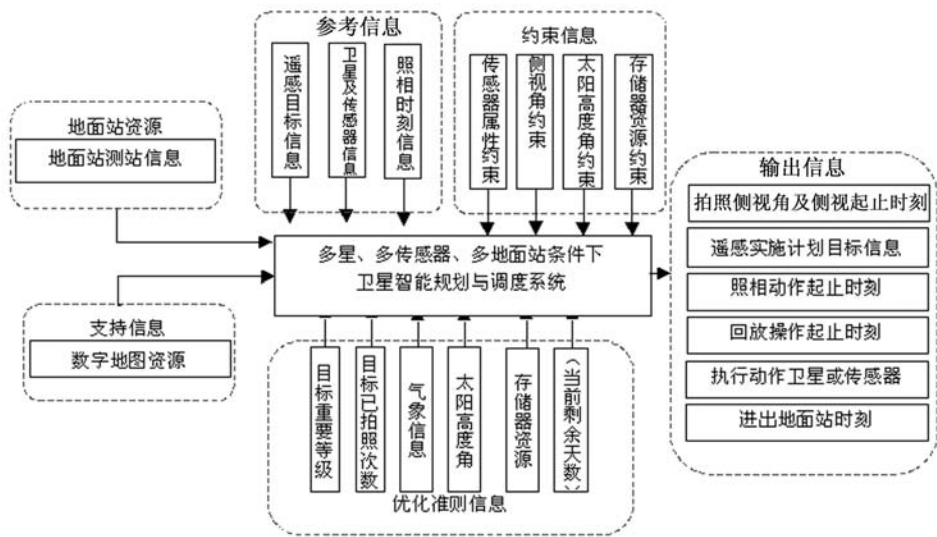


图 1 卫星遥感任务规划问题示意图

卫星遥感任务规划其主要任务是根据输入的卫星遥感参数、轨道预报等数据，计算卫星遥感计划预案及地面站测站计划，生成各卫星侦照时目标的太阳高度角、侧视角、拍摄时间以及进出地面站时

间，结合气象数据等信息，对可能的遥感实施方案，进行优化分析，辅助操作人员进行决策，形成遥感实施计划、地面站跟踪接收计划，并生成载荷控制指令

- 在规划过程中需要考虑以下目标因素。
- 1) 目标数量因素：主要考虑拍摄路径中的目标数目。
  - 2) 目标拍摄效果影响因素：主要考虑拍摄路径中目标的光照和气象条件优良的目标数目。
  - 3) 侧视次数或角度影响因素：主要考虑拍摄路径中总的侧视次数或角度。
  - 4) 重点保障目标数目影响因素：主要考虑拍摄路径中的重要目标的数目。

3 算法设计

遗传算法（GA：Genetic Algorithms）是寻求一种适合于大规模问题并具有自组织、自适应、自学习能力的算法，GA 将问题的求解表示成染色体的适者生存的过程，通过染色体群的一代代不断进化，包括复制、交叉和变异等操作，最终收敛到最适应环境的个体，从而求得问题的最优解。

从多星遥感任务规划的特点来看，规划结果需要满足相机开关机时间、卫星侧视时间、卫星侧视速度等多项严格约束条件，另外，要考虑胶片/存储器容量、卫星携带总气量、电力总量等能力约束；同时，由于待拍摄资源/目标分布可能极不均匀，某些地区目标数目众多，这样，造成该问题具有 NP-hard 特性。使用遗传算法求解卫星优化拍摄方案的流程如图 2 所示。

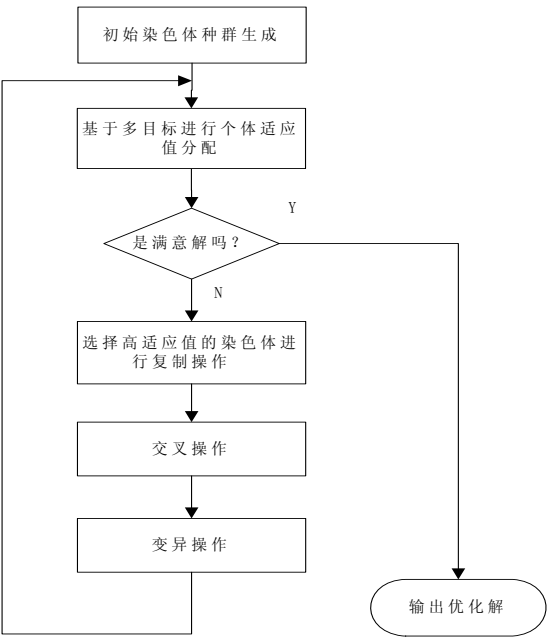


图 2 遗传算法求解卫星优化拍摄方案流程图

遗传算法将从一组随机产生的初始解，即“种群”出发开始搜索过程，种群中的每个个体都是问题的一个解，称为“染色体”，染色体在后续的迭代过程中不断进化，适应值高的个体保留下来，经过若干代以后，算法收敛于问题的最优解或次优解。其中涉及以下几个环节：参数编码、设定初始种群、设定适应值函数、复制、交叉、变异操作、算法控制。适应值是对染色体（个体）进行评价的一种指标，是进行优化所用的主要信息，它与个体的目标值存在一种对应关系；复制操作通常采用比例复制，即复制概率正比于个体的适应值，适应值高的个体在下一代中复制自身的概率大，从而提高了种群的平均适应值；交叉操作通过交换两父代个体的部分信息构成后代个体，使得后代继承父代的有效模式，从而有助于产生优良个体；变异操作通过随机改变个体中某些基因而产生新个体，有助于增加种群的多样性，避免早熟收敛。

4 算法要点

- 对于遗传算法，有以下主要的技术问题。
- 1) 遗传编码问题：就是将问题的解用一种码来表示，从而将问题的状态空间与遗传算法的码空间相对应，遗传算法的优化过程不是直接作用在问题参数本身，而是在一定编码机制对应的码空间上进行。
  - 2) 遗传操作问题：包括选择操作、交叉操作和变异操作等。
- 选择操作：有比例选择等多种方式。比例选择是以适应值的大小为比例进行遗传过程中的父体选择，被选中的个体作为父代参与后面的遗传操作以产生子代，也就是给那些处于优势的个体以更多的繁衍机会。
- 交叉操作：交叉操作用于组合出新的个体，在解空间中进行有效搜索。
- 变异操作：当交叉操作产生的后代适应值不再进化且没有达到最优时，就意味着算法的早熟收敛。其根源在于有效基因的缺损，变异操作在一定程度上克服了这个问题，有利于增加种群的多样性。

因此我们在以下方面做了深入研究。

- 1) 问题解的编码：卫星遥感任务规划与调度问题的解对应着一系列按时间顺序排列、满足各项

约束条件的待拍摄目标。

2) 解空间的分类: 对于遥感任务的规划解来说, 其实就是一个拍摄路径。拍摄路径可以分为以下几类。

只要是满足各种约束条件, 能够执行的拍摄路径都称为可行解 (拍摄路径)。

考虑多目标特性, 当没有其他可行拍摄路径在所有目标函数取值上均优于本可行拍摄路径, 那么将这样的解称为有效解 (拍摄路径), 或称为非支配解 (拍摄路径)。

在所有有效拍摄路径中融入用户或决策者的意图和优化策略后优选出来的解称为满意解 (拍摄路径)。

3) 初始种群的构建: 规划问题的解对应着一系列按时间顺序排列、满足各项约束条件的待拍摄目标。算法开始将首先构建可拍摄目标的拍摄约束图, 通过拍摄图中的路径产生目标队列。而初始种群则从目标拍摄约束图随机选取。

4) 对于约束的处理: 任何合理的解都必须符合卫星的使用和遥感约束。算法在执行过程中把规划问题的约束在状态的表达形式中体现出来, 并设计专门的算子, 使状态所表示的解在搜索过程中始终保持可行性。在遗传编码过程中不考虑约束, 而在搜索过程中通过检验解的可行性来决定解的弃用与否。图3给出了根据侧视约束构造的约束图。

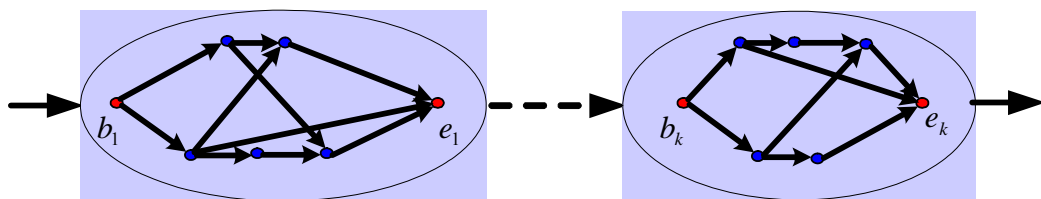


图3 侧视约束示意图

## 5 遗传算法的优化

### 5.1 优化方法

在实现过程中, 由于多星遥感任务规划问题涉及的决策因素很多, 加之构成解空间的基数变化范围很大, 我们发现采用通用的算法和约束条件进行规划时, 无法达到预期的效果。针对卫星遥感任务规划与调度问题的特点, 我们采取了有针对性的优

化方法。

1) 尽可能保持解空间的多样性。这里主要是让可行解尽可能的分布在整個解空间内, 避免整个算法过早的收敛在局部优化解上。为了保持解的多样性, 我们采去了两个办法。

使算法尽可能沿着非支配解边界维持种群。这样可以得到整个 Pareto 集合上的均匀采样, 使得优化结果具有更好的性能。具体如下图4所示。

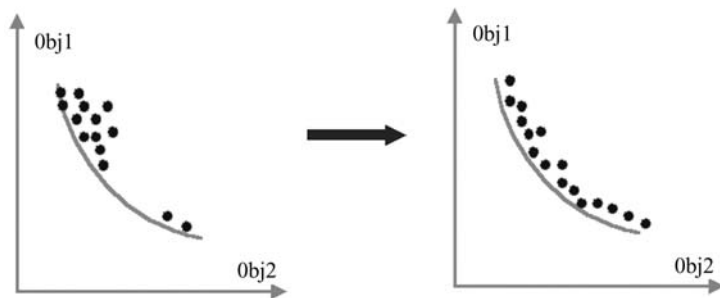


图4 非支配解边界维持种群示意图

采用优化的密度估计函数: 当目标空间中某点周围其他点较为密集时, 该点对应的个体适应值降低, 从而被选择参与遗传操作的概率将降低, 以避免很多无谓的遗传操作, 提高算法效率。主要使用了最临近法和核函数法。

2) 尽可能保持优良解。为了保持 Pareto 解能够加入某个第二种群, 在进化过程中需要维持一组非支配解, 以保证最后 Pareto 解集的多样性。另外由于存储容量限制及对算法效率的考虑, 第二种群数常不可能无限增长, 常常是有界的, 主要通过聚

类等技术予以解决。

3) 选择合适的适应值计算函数。适应值函数决定着算法何时结束。好的适应值函数应该在最恰当的时候结束算法，以避免浪费时间。对拍摄序列的好坏进行评价需要考虑多个准则的情况，进而确定个体的适应值。有多种方法进行适应值的分配，如排序法和距离法等。在本算法中，经过比较我们选择了距离法。在距离法中，可以根据距离度量方式确定与当前代理理想解最近的解，使用加权  $L_p$  范数作为距离度量方式：

$$r(\mathbf{z}; p, \boldsymbol{\omega}) = \left\| \mathbf{z} - \mathbf{z}^* \right\|_{p, \boldsymbol{\omega}} = \left( \sum_{j=1}^q \omega_j^p \left| z_j - z_j^* \right|^p \right)^{1/p}$$

其中  $(z_1^*, z_2^*, \dots, z_q^*)$  是判据空间的理想点，权重向量为  $(\omega_1, \omega_2, \dots, \omega_q)$ 。

个体的适应值定义为：

$$eval(\mathbf{x}) = \frac{r_{\max} - r(\mathbf{x}) + \gamma}{r_{\max} - r_{\min} + \gamma}$$

其中  $\gamma$  为  $(0, 1)$  之间的正实数， $r_{\max}$  表示当前代中的最大距离， $r_{\min}$  表示当前代中的最小距离。

5.2 优化结论

为验证上述优化方法对于卫星遥感任务规划与调度问题的优化效率，我们设计了一个观测实验。试验输入条件是选择 8 颗卫星、900 个目标和三个地面站参加任务规划，规划的周期是 5 个轨道圈次。使用 STK 进行轨道计算及成像角度预报。优

化前和优化后采用的输入约束条件完全相同。两个程序实验环境为 PentiumIV，512M 内存，Windows2000，程序使用 C++编写。

表 1 优化试验结果对照表

CPU 时间（秒）		优化前	优化后
进化代数	250	11.2	6.7
	500	34.4	28.9
	1000	134.7	60.2
	2500	429.4	167.3

通过试验结果我们发现，对于同样的进化代数（算法的循环次数），优化方法对于提高算法的时间效率是很明显的。同时随着进化代数的增加，其优化效果不论从绝对时间和优化比例来说都会更加明显。

6 结束语

利用遗传算法来解决多星遥感任务的规划问题是一个很新的研究方向。本文在分析遥感任务规划特点的基础上，讨论了遗传算法的实现方法，并对算法实现的流程、关键问题以及成像调度优化问题进行了输入讨论。通过理论分析和实验可以看到，遗传算法对于解决这类复杂问题是可行有效的，同时随着问题规模增大，本方法的优势将更加明显。但是本文只是在算法层面上进行了分析，而没有针对整个规划系统的工作模式和工作流程上进行分析和优化，这是在后续工作中需要解决的问题。

参考文献（略）

作者联系方式

通信地址：61646 部队  
邮政编码：100085  
联系电话：13141313888

# 基于WSN的自动数据采集和处理系统研究

陈贤明 李俊 蔡跃明 李宗海 曾文

**摘 要:** 无线传感器网络 (WSN) 综合了传感器、嵌入式计算、分布式信息处理和无线网络通信等技术, 可以实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息, 并对这些信息进行处理后传送给用户终端。文章介绍了无线传感器网络的概念、组成及军事应用, 提出了基于 WSN 的自动数据采集和处理系统方案, 最后针对 WSN 的应用特点, 研究了既能达到节能目的又有较好抗衰落作用的协同传输技术。

**关键词:** 无线传感器网络; 数据采集; 协同传输

## 1 概述

无线传感器网络从发展之初就受到了学术界和各大科研院所的高度重视, 美国商业周刊和 MIT 技术评论在预测未来技术发展的报告中, 分别将无线传感器网络列为 21 世纪最有影响的 21 项技术和改变世界的十大技术之一<sup>[1]</sup>。随着对该技术的深入研究和微型制造技术、无线网络通信技术以及电源技术的不断进步, 使得低成本、低功耗的微型无线传感器网络节点的大规模生产制造成为可能。

无线传感器网络集成了传感器技术、嵌入式计算技术、分布式信息处理技术和无线网络通信技术, 用户可以根据不同的需求采用相应的传感器, 利用飞机高空抛撒或者人工布设的方法放置到要监控的区域内, 从而实现对该区域内的各种环境或监测对象的信息进行实时监测、感知和采集, 并对这些信息进行处理, 传送到用户终端。

国外研究的起步比较早, 如美国交通部提出的“国家智能交通系统项目规划”、英特尔公司的“基于微型传感器网络的新型计算发展规划”等都已进入实际应用开发阶段, 加州大学等多所科研院所对无线传感器网络的协议、操作系统及系统进行了深入研究, 并取得了较大进展, 在军事上也开展了多个项目的研究。我国的清华大学、中科院传感器技术国家重点实验室以及部分军队院校等单位, 于 2002 年开始了传感器网络的相关研究, 取得了一定的成果, 但相对于发达国家来说还是有很大的差距<sup>[3]</sup>。

基于无线传感器网络的自动数据采集和处理系统是在军队信息化建设项目基金资助下开展的研究

课题, 本文提出了系统架构设计方案, 最后针对应用场景研究了无线传感器网络协同传输技术。

## 2 无线传感器网络的组成及军事应用

### 2.1 系统组成

典型的无线传感器网络体系结构包括分布式传感器节点 (群)、数据接收发送器 (Sink 节点)、远程连接设备 (网关) 和用于数据存储处理的数据库系统等<sup>[4]</sup>。其中, 传感器网络节点的基本组成和功能包括如下几个单元: 传感单元 (由传感器和模数转换功能模块组成)、处理单元 (由嵌入式系统构成, 包括 CPU、存储器、嵌入式操作系统等)、无线通信单元 (由无线通信模块组成)、以及电源部分, 网络及节点组成如图 1 所示。此外, 可以选择的其他功能单元包括: 定位系统、移动系统以及电源自主供电设备等。

### 2.2 军事应用

无线传感器网络最初的研究是应用于军事领域, 目前在军事和民用领域都有了广泛应用。民用方面主要有环境生态监测、交通控制、智能建筑和办公环境等, 在军事领域, 无线传感器网络将成为 C4ISRT (Command, Control, Computing, Communication, Intelligence, Surveillance, Reconnaissance and Targeting) 系统不可或缺的一部分, 如美陆军提出的“灵巧传感器网络通信”计划、“无人值守地面传感器群”项目、“战场环境侦察与

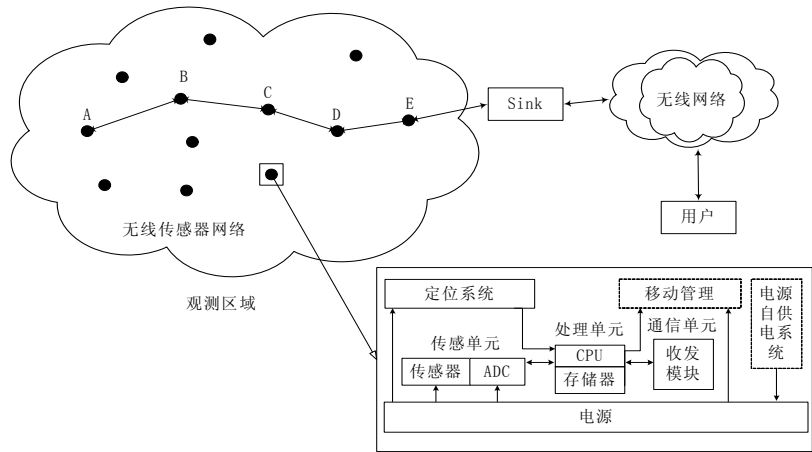


图1 典型的传感器网络系统结构和节点组成

监视系统”项目、以及海军的“传感器组网系统”研究项目等都体现了这一思想<sup>[3]</sup>。总的来说，无线传感器网络的作用主要可归纳为以下几个方面。

- 监测己方人员伤亡和装备损耗等情况：通过在人员、装备上附带各种传感器，可以让各级指挥员比较准确、及时地掌握己方的武器弹药消耗及人员伤亡情况，便于及时报告指挥所进行补给。
- 监测敌方的兵力部署及作战动态：通过在敌方阵地部署各种传感器，可以了解敌方兵力和武器装备部署情况，为指挥员确定进攻目标和进攻路线提供依据。在阵地前沿和作战要地部署大量传感器，可以及时发现敌军的作战行动，为己方提供准确的作战态势。并可根据战况快速调整和部署新的无线传感器网络。
- 评估战场情况：在攻击目标附近部署传感器网络，收集目标被破坏程度的数据。
- 核、生、化侦察：无线传感器网络可以实时监测区域内是否受到生、化武器的攻击，为决定

是否采用防护措施提供科学依据，并可对人员、装备的洗消情况进行监测。

- 采集训练和试验数据：在大型的训练基地或综合试验场部署无线传感器网络，可以采集弹着点、杀伤半径和装备动态跟踪等各种需要的参数，为作战效能评估提供所需数据。

### 3 基于WSN的自动数据采集和处理系统

系统设计的基本思想是在训练基地或试验场铺设大量的传感器节点收集信息，并对相关原始数据进行融合处理，再通过汇聚节点传送到中心数据处理设备，建立数据库系统以便于查询、管理和性能评估，从而提高评估的实时性、准确性和科学性，系统设计方案如图2所示。

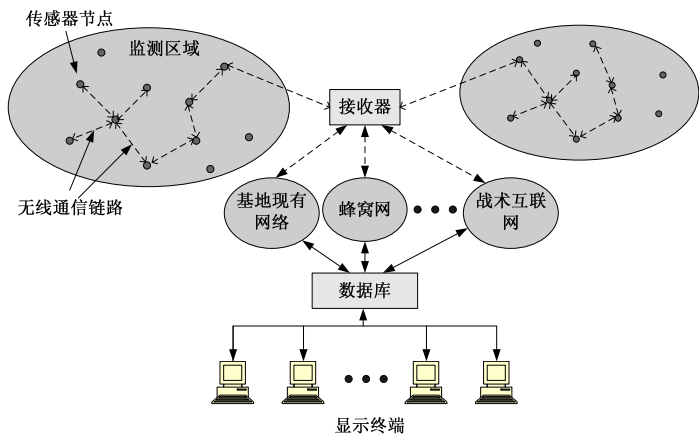


图2 系统设计方案

为了深入研究，解放军理工大学通信工程学院移动通信实验室研制了由少量节点组成的试验网

络。图 3 所示为网络节点外形，图 4 为在用户终端

显示的查询结果。



图 3 传感器节点

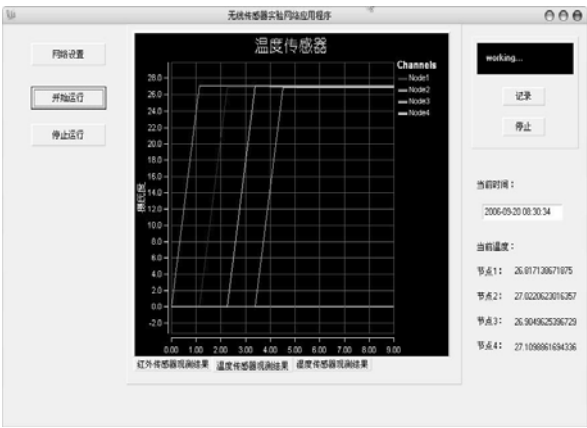


图 4 用户查询界面

在服务器端 PC 上创建一个数据库，并将采集到的数据收集、存储在该数据库中，同时架设网页服务器，利用动态网页连接该数据库，通过 ASP

动态网页实现了远程用户查询，该数据库支持数据的实时更新和多用户同时查询。图 5 为通过网络实现远程查询的显示界面。



图 5 远程网络查询动态网页

无线传感器网络节点体积小，单节点的数据存储、处理和电池能量有限。由于无线传感器网络节点数量大、分布广，而且往往部署在复杂环境条件下，特别是在军事应用中，网络节点通过更换电池的方式来补充能源是不现实的，因此，如何实现节约能量来最大化网络寿命是无线传感器网络面临的首要挑战。研究表明<sup>[5]</sup>，采用无线传感器网络协同传输技术既可获得较好的能量效率，同时又能起到较好的抗信道衰落作用。

#### 4 无线传感器网络协同传输技术

传统的节点能量管理策略<sup>[6]</sup>和基于节能的协议研究<sup>[7]</sup>在提高 WSN 能量效率方面取得了长足的进步，这些技术关注的主要是节点能耗问题，而对抗信道衰落、信道间干扰等问题缺乏有效的方法和手

段。在野外工作条件下，抗衰老、网络拓扑结构的鲁棒性恰恰是大规模 WSN 应用发展的关键与瓶颈，协同传输技术的引入，为解决这些问题提供了新的研究思路和解决方法。

无线传感器网络中的协同传输思想来源于多入多出（Multiple-input Multiple-output，MIMO）技术。MIMO 技术通过空时两维信号的联合处理，可以有效对抗和利用信道衰落，在不增加带宽的情况下，能显著提高系统性能与容量。由于受能量、体积和造价限制，在 WSN 节点上安装多个天线是不可行的，针对这一问题，有些学者提出了协同传输机制<sup>[8] [9]</sup>，其特点主要体现在两个方面：① 由一组单天线设备（分簇节点）构成虚拟天线阵列；② 用低成本单个设备获得 MIMO 信道高可靠性、高容量等性能。由于协同传输机制的组成、功能与通信方式与 MIMO 类似，因此也被称为虚拟

MIMO (Virtual MIMO) 或协同 MIMO (cooperative MIMO) 技术, 其典型结构如图 6 所示。在 WSN 中采用协同传输机制是一个较新的研究领域, 它来源于 MIMO 的思想, 信道估计、信道均衡等许多 MIMO 研究成果都可以被借鉴和使用, 但在技术特征和实现结构上并不等同于 MIMO 技术, 仍有许多问题亟待解决。

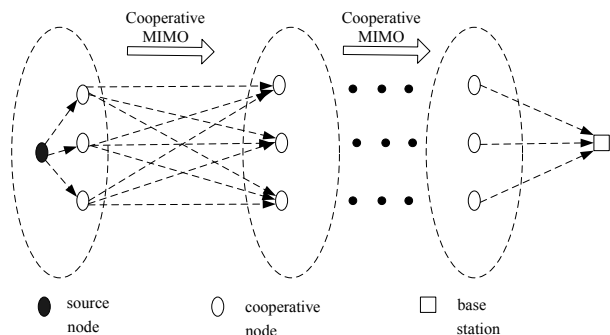


图 6 无线传感器网络协同 MIMO 结构

通过对协同 MIMO 传输的 WSN 性能分析可知<sup>[10]</sup>, 采用合理的分簇规模、最优协同节点选择和功率分配、分集与复用的折衷、优化设计传输方案

和高效的信道编码等技术, 协同 MIMO 传输系统就能够获得较好的分集与复用增益, 提高信道容量, 从而可以实现降低节点发射功率、减少能量消耗、延长网络生命期等目的。

## 5 结束语

由于具有覆盖区域广阔、监测高精度、可远程监控、可快速部署、可自组织和高容错性等特点, 无线传感器网络的应用前景非常广阔, 现在已经广泛应用于军事侦查、环境监测、动植物栖息地生态监测、健康护理、复杂机械监控和智能家居等诸多领域。无线传感器网络作为一门新兴技术, 从物理层到应用层都存在许多有待研究的问题, 本文主要针对无线传感器网络在军事方面的应用, 提出了一个包含数据采集、组网和远程查询的应用系统设计方案, 介绍了协同技术在无线传感器网络中的应用情况, 以期能对我们今后的研究起到一定的启发作用。

(本课题为江苏省自然科学基金 (BK2007002) 和军队预研项目 (XBLY-2007-120) 资助项目)

## 参考文献

- [1] 中国 ZIGBEE 联盟论坛, 传感器网络的背景、意义及研究内容, www.51zigbee.com. 2004.
- [2] Crossbow Technology Inc. Crossbow 2006 Wireless Sensor Networks Product Reference Guide. <http://www.xbow.com>, 2005.
- [3] 李建中, 李金宝, 石胜飞, 传感器网络及其数据管理的概念、问题与进展, 软件学报, 2003.14 (10), pp: 1717-1725.
- [4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci "A Survey on Sensor Networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp: 102-114, Aug. 2002.
- [5] S. Cui, A. J. Goldsmith and A. Bahai, Energy-efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks. *IEEE Journal on Selected Areas of Communications*, 2004, 22 (6), pp: 1089-1098.
- [6] Chien C, Elgorriaga I, Mc Conaghy C. Low- Power Direct - Sequence Spread - Spectrum Modem Architecture For Distributed Wireless Sensor Network. R. ISLPED '01, Huntington Beach, CA, 2001.8, pp: 251-254.
- [7] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy - efficient Communication Protocol for Wireless Microsensor Networks. R.Proc. 33rd Annual Hawaii International Conference on System Sciences, 2000, pp: 3005 -3014.
- [8] 赵海涛等, 协同传输机制在无线传感器网络中的应用及性能分析. 中国通信学会无线及移动通信学术年会, 2006, pp: 13-19.
- [9] X. Li, Energy efficient wireless sensor networks with transmission diversity. *IEEE Electronics Letters*, vol.39, Nov. 2003, pp: 1753-1755.
- [10] Wenyu Liu et al, Energy efficiency of MIMO Transmissions in WSN with Diversity and Multiplexing Gains. ICASSP 2005, pp: 897-900.

## 作者联系方式

通信地址: 南京市标营 2 号通信工程学院 邮政编码: 210007 联系电话: 025-80828394



# 战术互联网中基于MPLS实现HMIPv6的框架模型研究

杜金柱 蒋晓原 杜磊

**摘 要:** 论文首先介绍了战术互联网在战场环境下应用 IPv6 所面临的主要问题, 针对这些问题, 论文介绍了多协议标记交换 (MPLS) 和 HMIPv6 技术的基本原理, 并在此基础上给出了战术互联网工作在 MPLS 机制下的 HMIPv6 网络组成模型, 描述了该模型在战场环境下的工作原理。最后分析了 MPLS 架构下移动 IPv6 的技术优势并对其在复杂战场网络环境下战术互联网中的应用前景进行了阐述。

**关键词:** 战术互联网; MPLS; F-HMIPv6; MIPv6oMPLS; 框架模型

## 1 MPLS基本原理

MPLS 是属于第 2.5 层交换技术, 是集成式的 IP over ATM 技术, 它引入了基于标记的机制, 它把选路和转发分开, 由标签来规定一个分组通过网络的路径, 网络路由器只需要判别标记即可进行转发处理。卷标作为 IP 报头在网络中的替代品而存在, 在网络内部数据包所经过的路径中, MPLS 在数据包所经过的路径沿途通过交换卷标 (而不是看 IP 包头) 来实现转发; 当数据包要退出 MPLS 网络时, 数据包被解开封装, 继续按照 IP 包的路由方式到达目的地。

MPLS 网络包含一些基本的元素, 在网络边缘的节点被称作标签边缘路由器 (LER), 而网络的核心节点就称为标签交换路由器 (LSR)。LER 作为 MPLS 的入口/出口路由器, 执行全部的第三层功能以及由于运行标记分发协议 (LDP) 而产生的标记绑定功能。数据分组在 LER 处进行等效前传类 (FEC) 映射, 并分配一个固定长度的标记, 生成标记栈。LER 连接到网络内部的 LSR。LSR 执行标记交换, 在 LSR 处不再检查分组头, 只需对分组标记栈的顶部标记进行处理, 检索一个包含出口和新标记的标记表并用新标记替换旧标记完成标记交换。LER 和 LSR 之间的 LSP 通过 LDP 协议建立。在 MPLS 网络中完成的是 IP 包的进入和退出过程, LSR 节点在网络中提供高速交换功能。在 MPLS 节点之间的路径就是卷标交换路径 (LSP)。一条 LSP 可以看作是一条贯穿网络的单向隧道。

MPLS 作为第三代网络技术, 支持 VPN 和流量工程, 因此 MPLS 越来越受到人们的重视, 如在

光网和传输网的应用 GMPLS, 在无线移动通信的应用 WMPLS 等。

## 2 F-HMIPv6 基本原理

移动 IPv6 为移动节点的通信提供了基本的保障, 解决了在移动 IPv4 通信中的三角路由、安全性和 QoS 保障问题, 但是存在路由开销和切换延迟大等问题。因此, IETF 提出了一个层次型移动 IPv6 微移动性管理方案 (HMIPv6)。HMIPv6 通过引入一个新的网络功能实体移动锚点 MAP, 负责处理移动节点在其位置管理域内的移动。当 MN 在 MAP 域内发生位置切换时, MN 的位置注册消息由 MAP 处理, 可以有效减少 MN 与 HA 和 CN 之间传输距离较长的位置注册信令交互数量, 将位置注册信令负荷限制在局部网络范围内。这样, 全网范围内的位置注册信令负荷明显减少, 切换性能也能得到有效改善。

在 HMIPv6 中, 当移动节点 MN 进入一个 MAP 域中时, 它会收到包含一个或多个 MAP 选项的路由器公告。MN 从中选择一个为自己服务, 并形成新的 RCoA 和 LCoA。之后, MN 先向 MAP 发送 LBU 以注册 RCoA 和 LCoA 的绑定, 然后向 HA 和通信对端 CN 注册 RCoA。这样, MAP 就会代替 MN 接收来自通信对端的数据分组, 并通过隧道将它们转发到 MN 的 LCoA。如果 MN 在域内移动, 它只需向 MAP 注册新配置的 LCoA, 而 RCoA 保持不变。

每一次检测到移动, MN 都会检查原来的 MAP 选项是否被包含在新接收到的路由器公告

中,以判断自己时候还在原来的 MAP 区域内。如果原 MAP 不再有效, MN 必须重新选择一个 MAP、配置新的 RCoA 和 LCoA,并向新的 MAP 注册。此外, MN 还要向 HA 和 CN 注册新的 RCoA。由于战术互联网是采用分层的网络结构,因此,基于分层概念的 HMIPv6 在战术互联网中将是其主要的应用模式。

快速切换层次移动 IPv6 (F-HMIPv6) 是将 HMIPv6 和 FMIPv6 相结合,利用 HMIPv6 的层次结构进一步降低了 FMIPv6 的切换延迟。与 FMIPv6 不同的是, F-HMIPv6 使用链路层机制检测到新的接入路由器,并通过预先注册来降低切换延迟。它是在 MAP 和 NAR 之间建立快速切换的分组转发隧道。为此,移动节点和 MAP 交换快速切换消息。F-HMIPv6 仍然使用 FMIPv6 中的消息完成快速切换,不必定义新的消息。

### 3 战术互联网环境中基于MPLS机制的F-HMIPv6 的框架模型

传统的移动 IP 协议是一种支持一定节点大范围移动的网络层方案,但其存在移动节点与其家乡代理的信令负荷过重,切换过程中时延较大。分组丢包率较高,容易造成连接中断等问题。MPLS 协议具有高速交换、QoS 保证、支持流量工程和快速重路由等特点,但不支持移动性。

MPLS 在 Frame Relay 及 ATM Switch 上结合路由功能,数据包通过虚拟电路来传送。它整合了 IP 选径与第二层标记交换为单一的系统,因此可以解决 Internet 路由的问题,使数据包传送的延迟时间减短,增加网络传输的速度,更适合多媒体信息的传送。

MPLS 的 LSP 支持软切换, LSP 只在网络入口 LER 进行一次 IP 数据包的等效前传类分配和标记映像,核心节点只作标记交换,简化了路由器对 IP 数据包的处理; MPLS 节点上的 FIB (前转信息库) 还可集成移动功能。MPLS 在保证无连接 IP 网络连接有效性的同时,能提供面向连接的网络服务。对于差分 MIP 业务, LSP 可提供适当的 QoS 路径。

MPLS 与移动 IPv6 的结合,可以改善移动 IPv6 在微移动性方面的性能,而 MPLS 域内的二层移动在切换时无管理开销,从而实现快速切换。

移动 IP 与 MPLS 技术的结合,不但可以通过移动 IP 技术使得 MPLS 网络提供对移动性的支持,而且可以通利用 MPLS 快速分组交换机制降低移动节点切换延迟和核心网络信令负荷及分组丢失,利用 MPLS 路径保护和快速恢复机制改善网络的可靠性,利用 MPLS 对流量工程和 QoS 的支持能力提高网络利用率以及对特定业务提供合适的 QoS 保证。

MIPoMPLS 的基本原理是 MPLS 上采用 LSP 隧道方案支持移动 IP 业务,由 MPLS LSP 实现 QoS 保证的路径,移动性检测由 L2 交换完成,切换快速、管理简单。当发生全球移动时,由 MIPv4/v6 完成,这时 LER 作为边界网关,具有 HA/接入路由器的功能。

当 MN 移动到新的接入点 (接入 LER) 时, MIPv6 节点的转交地址 CoA 发生改变,为了避免三角路由, MN 必须通过该接入点给家乡代理 HA 和通信节点 CN 分别完成绑定更新过程,然后,移动节点的 HA 和 CN 都将更新自己的绑定缓存表。

CN 得到 MN 的注册信息和请求信息以及 MN 的转交地址 CoA 后,查找其标记栈,并把 MN 的家乡地址作为 FEC; CN 根据 LDP 为 HA 到接入 LER 的路径分发标记,并向接入 LER 发送标记请求信息,把 MN 的 CoA 作为 FEC。接入 LER 收到标记请求信息后,向 CN 返回标记匹配消息, CN 收到标记匹配消息后更新其 MN 在标记中的注册信息。CN 通过 LSP 向接入 LER 发送注册响应信息,接入 LER 收到注册响应后,更新其标记栈,并增加接入 LER 到 CN 的 LSP 信息,注册成功,这样就在 CN 到接入 LER 之间建立起一条 LSP。此后移动节点与任意通信节点发送的数据报都将直接通过 LSP 到达通信 CN。

在 F-HMIPv6 环境中,当移动节点在一个 MAP 域内的接入路由器 AR 间移动时,移动节点仅需向 MAP 进行注册,原有的转发路径 LSP 不发生改变。当移动节点在不同的 MAP 域之间移动时,才需向 HA 和 CN 发送绑定更新消息,数据转发路径需要采用重路由机制进行更新。对于 HA、CN 和 MPLS 转发路径来说,移动节点在 MAP 域内的移动时透明的。

基于 MPLS 在战术互联网中实现 F-HMIPv6 的网络框架模型如下图所示。

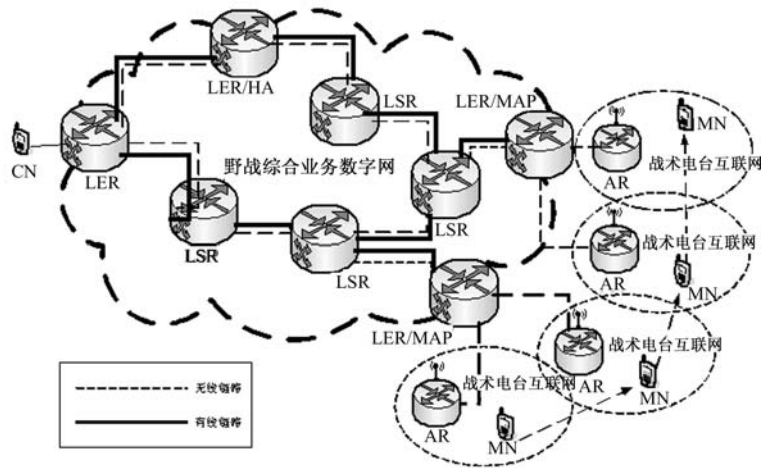


图1 战术互联网环境下中基于 MPLS 机制的 F-HMIPv6 的框架模型

## 4 战术互联网中MPLS与F-HMIPv6结合的优点

MPLS 与 F-HMIPv6 结合网络结构不仅使得移动节点在较大范围内移动的性能得到改善, 也为移动节点实现小范围快速无缝移动提供了保证, 因此, 本文建立的这个模型相比传统的单纯的的网络结构其优越性主要表现在快速切换、QoS 保证和支持移动状态下的 VPN 等。克服了战术互联网在战场环境中应用移动 IPv6 存在的主要问题。

- MPLS 架构下的移动 IP 技术集成了移动 IP 的高移动性和 MPLS 高速交换特性: MPLS 交换比 IP 路由由协议传输分组速度明显提高, 传输时延和数据包处理时间明显降低; 并且 HA/CN 到接入 LER 建立了一条 LSP, 数据报头过长问题得到解决。

- 提高了网络的安全性和支持 QoS: 在同一 MPLS 域中, 不再需要 IP-in-IP 方式传送数据包, 而是采用 MPLS 交换方式通过 LSP 传送数据包。整个传输过程都是在 MPLS 交换层进行, 不涉及 IP 层的路由协议, 从而提高了数据包的传输速率和移动 IP 的可扩展性, 为网络的 QoS 提供了保障,

并且网络的安全性能得到提高。

- 支持移动状态下的 VPN 和流量工程: 由于 MPLS 技术对 VPN 和流量工程都有很好的支持, 因此, MPLS 与移动 IP 的结合, 对移动状态下 VPN 和流量工程解决带来了希望。

## 5 结束语

移动 IPv6 是为战术互联网提供战术终端移动性的解决方案。由于未来战场网络的用户和移动终端数将非常庞大, 因此移动 IPv6 的可扩展性非常关键。本文通过将移动 IPv6 技术与 MPLS 技术相结合构建的基于 MPLS 机制的 F-HMIPv6 的框架模型, 通过高效、快速的 MPLS 骨干网络实现大规模的移动 IPv6 网络, 通过利用 MPLS 网络不同路径可以具有不同 QoS 性能的特性, 实现区分服务质量的移动 IP 业务。反之, 移动 IP 与 MPLS 的融合方案也为 MPLS 提供了移动性支持。因此, 本文提出的这个框架模型为战术互联网在复杂战场环境下应用 IPv6 协议提供了一个重要思路和技术方案。

## 参考文献

- [1] 石晶林, 丁炜. MPLS 宽带网路互连技术. 北京: 人民邮电出版社, 2001.3
- [2] 曲岩栋, 陈山枝, 金跃辉. MPLS 支持移动 IP. 中国通信学会信息通信网络技术委员会 2003 年年会, 2003.9
- [3] 王玉峰, 王文东, 程时瑞. Mobile IP 与 MPLS 集成的研究. 计算机工程与应用, Issue:6, Page:23-25, 2003.6

## 作者联系方式

通信地址: 北京市丰台区大成路 13 号 Z00 邮政编码: 100039 联系电话: 010-66820166

# SOA技术及对军队信息化建设的启示

胡博 陆余良 徐新华

**摘 要:** 面向服务的体系结构 (Service-Oriented Architecture, SOA) 作为信息领域的一门新兴学科, 在军事领域有着广阔的应用前景。文章介绍了 SOA 技术的相关概念、基本原理、运用优点及在军事领域中的应用。

**关键词:** 信息化; 体系结构; 服务

军事信息系统是军队信息化的主体, 是实现作战指挥信息化的主要手段, 搞好军事信息系统体系结构设计, 这要求武器装备系统、侦察监视系统、指挥控制系统、辅助决策系统等诸平台实现信息的无缝连接。美军从 20 世纪 90 年代后期开始的大规模信息系统综合集成的研究与实践, 最具有代表意义的工作主要是包括公共操作环境 (COE)、高层体系结构 (HLA) 和全球信息栅格 (GIG)。这三项被视作美军信息技术整合军事资源的核心工作, 为实施“网络中心战”奠定了较为坚实的基础。各军兵种内部的指挥管制, 跨军兵种之间的协同配合, 要求作战业务的流程迅速、快捷, 然而我军现实的情况是由于不同部门信息系统建设的独立性、建设标准的差异性、技术系统的离散性, 不同系统间的数据信息不能共享, 信息出现脱节, 即产生“信息孤岛”。“信息孤岛”的问题严重影响了军队整体的信息化建设过程, 军队各部门迫切需要一整套从信息获取、信息处理到信息传递与共享的解决方案。

## 1 SOA相关概念

面向服务的体系结构 (Service-Oriented Architecture, SOA) 是一个组件模型, 它将应用程序的不同功能单元 (称为服务) 通过这些服务之间定义良好的接口和契约联系起来。其中服务是封装成用于业务流程的可重用组件的应用程序函数, 它提供信息或简化业务数据从一个有效的、一致的状态向另一个状态的转变。而接口是采用中立的方式进行定义的, 它独立于实现服务的硬件平台、操作系统和编程语言, 这使得构建在各种各样的系统中的服务可以以一种统一和通用的方式进行交互。

著名科学家钱学森早在上个世纪八十年代就提出, 运用信息技术对现有军事资源进行“整合”, 通过系统集成、综合集成方法, 解决结构复杂、因素众多、目标多样的大系统, 明确提出了综合集成思想。就是说, 综合运用信息技术, 通过综合集成方法, 拆除“篱笆”、整合“烟囱”, 对结构复杂、接口不一的大系统, 实施有效“功能提升”, 并通过运用内部渗透、外部融合, 加速对现有装备的改造式集成, 最终达成整个庞大系统作战效能的整体跃升。研究表明, 运用面向服务的体系结构技术可以使武器平台之间实现横向组网, 并融入到信息网络系统, 做到诸军兵种作战信息资源共享, 从而有效提高武器平台的作战效能。因此, 加强面向服务的体系结构技术研究, 对军事资源整合, 推进我军信息化建设进程具有重要得意义。

## 2 SOA运用的基本原理

面向服务的体系结构提出将应用程序的不同功能单元都以服务加以描述, 使服务请求者能够更好的理解服务, 通过这些服务之间定义良好的接口和标准将不同服务联系起来。接口是独立于实现这些服务的硬件平台、操作系统和编程工具的, 这就使得构建在不同系统中的服务可以一种统一和通用的方式交互。这些服务的关键是它们的松耦合特性, 服务的接口和实现相独立, 应用开发人员可以通过组合一个或多个服务来构建应用, 而无需理解服务的底层实现。它的思想很简单, 让业务应用不受限于技术, 让开发方和使用方轻松应对不停变化的信息和业务需求。

SOA 是一套体系结构, 它模型可用图 1 表示。

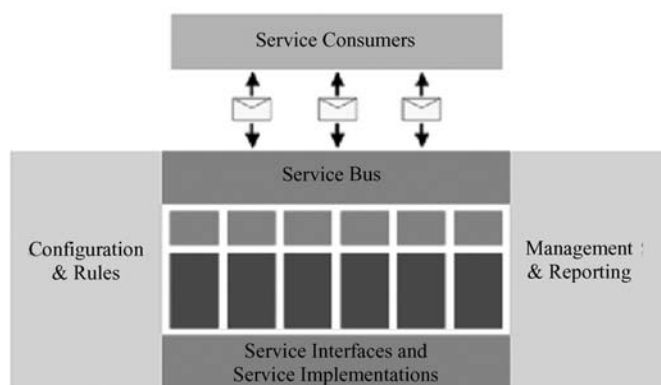


图1 SOA 体系结构图

SOA 服务用消息进行通信，该消息通常使用 XML Schema 来定义（也叫做 XSD，XML Schema Definition）。在服务描述中，XML 模式是基本数据类型的机制，所有服务描述技术都使用 XML 来表示。消费者和提供者或消费者和服务之间的通信多见于不知道提供者的环境中。服务使用方（Service Consumers）可以通过发送消息来调用服务，这些消息由服务总线（Service Bus）接收，并根据管理配置，通过服务接口（Service Interfaces）提交适当的服务实现。服务接口具有平台无关的特性，在这种接口之上的服务之间表现出松耦合的结构关系。松耦合的好处是使 SOA 具有业务灵活性，当一个服务的实现发生改变或者更新后，只要接口保持不变，就不影响其他服务对它的调用。这种松耦合结构需求来源于业务应用程序需要根据业务的需要变得更加灵活，以适应不断变化的信息资源和应用环境。比如经常改变的人事关系、政策法规等等与业务有关的因素，这些因素处理的不及时甚至可能影响业务的性质。这种能够灵活的适应环境变化的业务称为按需业务，在按需业务中，一旦需要，就可以对完成或执行任务的方式进行所需的更改。

SOA 的业务灵活性使用户可以快速构建、部署、整合已有的服务，且无需依赖应用程序和运行平台，可使用户加快信息系统发展速度、降低总体成本，改善对信息的及时、准确处理能力。

### 3 SOA运用的优点

在我军信息化改造过程中采用面向服务体系结构将给我们带来诸多方面的好处，更有利于对现有军事资源进行“整合”。

**以服务为中心的体系结构。**在以服务为中心的

体系结构中，通过将注意力放在服务上，使业务应用开发摆脱面向技术束缚，它从业务流程的角度来看待技术。定制服务的过程就是将变化的部分与稳定的部分区别开来，流程控制变化的部分，服务概括稳定的业务模型部分。以服务为中心的优势很明显：它能更好的同业务流程相结合，因此能够更加精确地表示业务模型、更好的支持业务流程。

**减少成本。**随着业务需求的发展和新的需求的引入，通过采用 SOA 及其服务库，通过把服务联系起来而不是编写新的代码来构架新的应用，为用户现有信息化资产带来了更好的重用性，降低总体改造成本。这种机制的应用尽量避免大规模的新的代码的开发，广泛发挥每个已有服务的价值。

**更快的响应。**通过现有的服务组合新服务的能力为那些需要灵活响应的组织提供了帮助。利用现有的组件和服务，可以缩短软件开发生命周期（包括收集需求、进行设计、开发和测试）。

**降低风险。**重用现有的组件降低了在创建新的业务服务的过程中带来的风险，这也减少了维护和管理支持服务的基础架构的风险。

**更易于集成和管理。**在面向服务的体系结构中，集成点是规范而不是实现。这提供了实现的透明性，并将因为基础设施和实现发生的改变带来的影响降到最低限度。通过提供针对基于完全不同的系统构建的服务规范，使应用集成变得更加易于管理。特别是当多个单位一起协作时，这会变得更加重要。

**持续改进业务流程。**SOA 允许清晰地表示流程流，这些流程流通过在特定的业务服务中使用的组件的顺序来标识，这给用户提供了监视业务操作的理想环境。业务建模反映在业务服务中，流程操纵是以一定的模式重组部件来实现的。这将进一步

允许更改流程流,而同时监视产生的结果,因此促进了业务流程地持续改进。

## 4 SOA给军队信息化建设的启示

随着现代化军事变革的深入,军队各部门日常的业务也在不断改变、更新、信息量越来越大。而战时各军兵种、各级作战单位的指挥控制系统在处理战场瞬息万变的信息时,战略的调整、战术的制定,更需要敏捷、稳定、高效地获得信息和服务。需要针对这些变化进行快速部署和行动,这受许多因素的影响。比如掌握信息量不够,辅助决策不充分等,但最大的难点莫过于协调和优化各单位,各业务系统之间的关系。

SOA 提供了一种机制,通过这种机制,可以不区分实现的平台或语言地集成现有的遗留应用程序,从而形成松散耦合的系统。松耦合系统的好处有两点:一是它的灵活性;二是当组成整个应用程序的每个服务的内部结构和实现逐渐地发生改变时,它能够继续存在。SOA 为上文所述的那些问题提供了良好的解决方案,在军用信息系统开发中,逐步采用 SOA 这一体系结构。使军队各单位内部、总部与基层之间、陆、海、空、天、电、网等各个战场空间的信息系统协调一致,提高信息系统的生存能力,保证信息的畅通,为全军信息化建设提供可靠支持。

SOA 在军队真正走向应用,还需要许多工作要做。

第一是安全问题,由于灵活的共享机制,很多情况下需要把服务暴露在外,导致服务的安全问题非常重要。SOA 可显著改善业务的灵活性和敏捷性,但它必须首先是安全的。

第二是标准问题,SOA 的建立需要所有指定

的服务和接口具有一个统一、规范的标准。和基于 XML 技术的 Web Service 技术一样,如果没有标准,SOA 也无从谈起。全球 IT 企业目前对商用 SOA 的标准正在研究中,合适的军用标准应该建立在商用标准之上,使之更符合军队实际。

第三是技术业务复合型人才的培养,这种复合型人才是实现 SOA 的重要组成部分。SOA 强调从业务流程的角度制定服务,这就需要有熟悉军事单位种种也为的技术人员,一方面他们要熟悉诸如 IBM、BEA、Oracle、Microsoft 等不同商用 SOA 解决方案中的众多基础设施的产品(从业务分析、建模、开发、部署、测试的一系列),另一方面要了解业务模型、熟悉业务流程可能产生的变化等等。

SOA 作为一种刚刚兴起的技术,虽然有一定的不确定性,但是这并不能阻碍 SOA 技术的不断发展。随着互联网络的进一步发展,分布式信息化战场上应用的不断普及,SOA 的应用会更加普遍并被人们所接受,成为继面向对象、面向组件之后的新的设计方式。因此可以预见,SOA 的未来高科技战争的作战思想产生巨大的影响。

## 5 结束语

SOA 是一套体系结构,也是一种开发方法论,它的宗旨在于使信息系统变得更加敏捷,共享更加方面,信息获取、处理、分发过程更加快捷、可靠。对于军队信息化建设来说,这是一种新事物、新变化,同时也是一种挑战。我们只有着眼于争夺信息优势,构建互连、互通、互操作、无缝连接的综合信息系统,才能为多军兵种联合作战提供一体化信息支持。

### 参考文献(略)

### 作者联系方式

通信地址:安徽合肥黄山路 460 号电子工程学院研三队

邮政编码:230037

联系电话:13866716166 0551-5767844

# 移动GIS的新应用——位置服务技术

贾艳

**摘 要:** 本文简要介绍了移动通信位置服务(LBS)的概念、系统组成、定位技术、应用范围;以及移动通信位置服务的发展现状、我国移动通信位置服务产业存在的问题和据此提出的建议。

**关键词:** GIS; LBS; 移动通信

## 1 引言

随着移动通信技术、地理信息系统技术和互联网技术的结合,移动GIS已经进入人们的生活,并将会得到不断的发展,为用户提供广泛的服务。同时,GIS与电信运营系统的结合,由为用户提供位置信息服务,发展为一门新的GIS分支——基于位置的服务(LBS—Location Based Services)。

## 2 LBS的概念

LBS是由移动通信网提供的一种增值业务,通过一组定位技术获得移动台的位置信息(如经纬度坐标数据),提供给移动用户本人或他人以及通信系统,实现各种与位置相关的业务。狭义地说,LBS业务是通过无线通信网络获取无线用户的位置信息,在GIS平台下支持提供相应服务的一种无线增值业务。广义地说,是基于位置的信息服,有些业务与位置无关,如固定地点的天气、固定起始终止点之间的公交线路等。我国移动电话的数量已经成为世界第一,LBS服务几乎涵盖了人类动态活动的每一方面。可以预测LBS在我国将是一个新的GIS热门领域。

## 3 LBS系统组成

LBS系统由数据平台、移动通信网络、位置确定中心、位置服务平台、运营服务平台和移动信息终端等设备组成。

其中位置确定中心的作用是从基站获取数据并计算出位置信息,接受移动信息终端的位置请求并返回其位置信息;而位置服务平台则是根据位置确

定中心提供的用户位置信息,与其他相关信息相结合,提供一种基于位置的综合信息服务,它是整个LBS系统的关键环节。

在空间位置服务平台中GIS平台承担了空间信息管理、查询、分析等主要工作,是空间位置服务系统的核心。优秀的GIS平台和技术及移动通信运营商是构建基于手机的位置服务的应用系统的坚强基石。2006年中国联通开发的“企业之星”定位系统就是在国产大型平台——MAPGIS上进行二次开发并结合了基于CDMA网络的GPSOne定位技术开发出来的,已经在全国多个城市进行了分布式的部署和业务接入,系统均衡负载能力强,整体运行稳定,收到了较好的社会和经济效益。

## 4 LBS的定位技术

### 4.1 基于CELL ID

适用于所有的蜂窝网络,在网络侧增加简单的定位流程处理即可。它的定位原理:网络根据移动台当前的服务基站的位置和小区覆盖来定位移动台。

### 4.2 应用于3G网络下

定位的基本原理是:移动台测量不同基站的下行导频信号,得到不同基站下行导频的到达时刻,即所谓的导频相位测量。根据该测量结果并结合基站的坐标,采用合适的位置估计算法,就能够计算出移动台的位置。

### 4.3 网络辅助的GPS

这种方法需要网络和移动台都能接收GPS的

信息。它的原理是：网络向移动台提供辅助 GPS 信息和移动台位置计算的辅助信息。利用这些信息，移动台可以很快的捕获卫星，并接受到测量信息，然后将测量信息发送给网络中的定位服务中心，由它计算出移动台当前所处的位置。

## 5 LBS的具体应用

### 5.1 查询本人或他人的位置

定位终端用户可以查询自己的位置信息，并可以将从 GIS 得到的位置信息发送给相应的手机终端。在对方允许情况下，用户可查询他人的当前位置。

### 5.2 导航服务

用户输入目的地地址，定位系统可以自动测出两点之间的距离并给出行进路线信息，可以实时指导用户按正确的方向行进。

### 5.3 特殊群体跟踪

个人用户包括小孩、老人、病人等需要特殊照顾的人员，通过特殊的终端可以向监护人发送告警信息，并告知监护人当前用户的位置。

### 5.4 事故紧急呼叫

当发生事故时，用户可启动紧急呼叫，将自己的位置报告给服务中心，由服务中心根据 GIS 提供的地图信息提供援助服务。

### 5.5 汽车保险业务

运营商可以与保险公司合作。当汽车失窃时，保险公司可通过 GIS 对失窃车辆的位置进行查找，有利于降低车辆失窃险种的保费与吸引投保的客户群。

### 5.6 移动黄页

根据用户的位置信息，业务提供者可以将用户需要的信息发送给用户，例如查询最近的餐馆、ATM 机、交通等。移动黄页最直接的好处是用户能自动找到离自己最近的感兴趣的地方，而不必

输入具体的地址和邮编。尤其当你不知道这些时，这不单简化了用户的使用复杂度，也增加了该应用服务的使用量。例如，上海移动甚至已经开通了“厕所查询系统”，用手机报出你所在的方位，该查询系统就能给你提供“导厕”服务。

以上的各项应用借助于 GIS 强大的地图表现能力、路径搜索能力和地理编码等功能，可以使用户获得优质的基于位置信息的各项增值服务。正是有着上述丰富的业务和技术优势，GIS 成为位置服务业务的重要支撑平台<sup>[1]</sup>。

## 6 LBS的发展现状

### 6.1 国外LBS的发展

近年来伴随着移动通信网络从 2.5G 向 3G 的演变，从日本、韩国到欧美地区，移动通信业务的发展步伐在不断的加快。2003 年全球 LBS 业务的市场规模约为 50 万美元，2004 年为 100 万美元，据亿舟咨询估计，到 2009 年，全球 LBS 业务的市场规模可达到 2100 万美元。

现阶段美国、欧洲运营 GSM 网络的移动公司所采用的移动定位技术基本以 CELL ID 为主，所能实现的定位精度可以满足大部分应用的要求，进入和使用门槛相对较低。

与欧美相比，日韩在 LBS 的商业应用方面较为领先，这得益于日韩在 3G 方面的快速发展。其特点有如下几个方面：第一，不断进行技术升级，提高定位精度。韩国和日本先从 Cell ID 开始，但由于定位精度不高，能提供的内容非常有限，因此发展的用户也很少；随后运营商不断升级技术，比如日本 NTTDoCoMo 于 2000 年 1 月推出了采用 GPSone 技术的“DoCoNavi”移动定位服务，韩国 SK 电讯在 2002 年 7 月正式推出了基于 GPS 的名为“NATEGPS”的位置服务业务。目前日韩运营商几乎都采用 GPS 定位技术，定位精确度非常高，内容越来越丰富，深受用户欢迎。第二，联合 SP 建立移动位置门户，为用户提供丰富的信息服务。为推动位置服务业务的发展，韩国和日本的运营商建立了门户网站，吸引了众多 SP，推出丰富的位置服务内容。如 NTTDoCoMo 推出的基于 i-Mode 品牌的定位服务“iArea”，提供的内容包括 WNI 气象信息、iMapFan 电子地图、美食家、



ATIS 交通信息、Zenrin 便携式地图以及住宿信息等 6 项服务；KDDI 推出的定位业务已达 100 多种，如电子地图、餐馆指南、火车时刻表、城市指南、天气和紧急信息等；2003 年 3 月，VodafoneK.K 推出了名为“LocoGuide”的移动门户。通过“LocoGuide”门户，用户可以得到许多基于自身位置的信息，如交通信息、最近的餐馆、休闲场所、银行、医院等的位置信息。第三，注重终端的配合。利用 GPS 技术的位置服务需要终端的大力支持，否则业务发展只是空话。日本 KDDI 在 2002 年 12 月推出了采用高通 GPSOne 技术芯片组的终端，从而可以全面支持“轻松导航”业务，生产这种手机的厂商包括日立、京瓷和东芝。截止到 2005 年 6 月，KDDI 所售的手机中 70% 支持 GPSOne 移动定位技术，而且这些机型的价格在 200 美元以内<sup>[2]</sup>。

## 6.2 中国LBS的发展

中国最早引入移动定位服务是在 2001 年，北京移动率先推出基于移动梦网卡的移动定位服务，随后各省陆续推出。2003 年 7 月，中国联通推出定位之星业务，该业务可以帮助家长通过手机 WAP、互联网查询、短信查询等方式随时了解孩子所处的方位。北京移动则推出了“亲子通”与之类似的位置服务业务。2005 年 10 月联通高调推出 114 汽车语音导航计划，与此同时中国移动正谋划 LBS 全面战略，加紧升级各地网络，以便在 2006 年春节前后实现全国 20 余省市联网提供手机信息服务，不过还未实现。

## 7 我国LBS产业存在的问题

第一，目前采用的定位技术主要是 Cell ID，定位的精度较差；第二，运营商网络带宽太窄，如

参考文献（略）

### 作者联系方式

通信地址：北京市北三环中路 69 号 5 分箱  
 邮政编码：100088  
 联系电话：010-66722225

果通过手机上网方式查找位置信息，传输速度和稳定性就成了很大的问题；第三，与定位密切相关的基站数据，运营商还不能做到及时更新，直接影响了定位的准确性；第四，GIS 的不统一，对同一经纬度的地理地址解释不同，影响了定位信息的准确性；第五，终端方面还不成熟，能够支持 A-GPS 或 GPSone 技术的终端在国内还比较少，价格也较昂贵。对于第一点和第二点问题，联通依靠 CDMA1X、BREW 和 GPSone 定位技术很好地给予了解决，定位精度要比移动做的好得多。但是后三点问题却是困扰两大移动运营商的共同问题，这些问题不仅影响了定位的精度，同时也削弱了用户使用业务的激情。

## 8 对我国LBS产业发展的建议

第一步，“立足现在，有的放矢”。主要是在近期，充分利用现有的 Cell ID 定位技术，为特定的个人用户提供简单标准化的位置查找和日常生活信息，比如查找小孩、老人的位置等。比如北京移动开展的“亲子通”业务，四川移动开展的“爱贝通”业务等等。这样一方面培养价值链，另一方面培养用户对位置服务的使用习惯。

第二步，“演进技术，全面开花”。主要是在远期，升级定位方式，发展基于 A-GPS 或 GPSone 的位置服务，形成多层次的位置服务体系。在升级定位技术的同时，运营商需要花大力气联合 SP 开发内容，建立位置服务门户网站。初期的内容可以包括一些常用的位置信息，比如餐馆位置信息、ATM 机位置信息、公交车位置信息等。让用户可直接通过手机上网，到门户网站上下载相关的地图，然后通过位置服务业务，了解基于位置的各种附加信息。当然，运营商也需要关注终端的发展，利用 3G 契机，提高手机对位置服务的支持比例<sup>[2]</sup>。

# 山区宽带移动战术通信的关键技术

蒋晓红 吕东强 詹平

**摘 要:** 本文对山区宽带移动战术通信的应用条件、传输要求、业务和使用情况等需求进行了描述,在此基础上,对解决山区宽带移动通信可以采用的关键技术进行了介绍,并简要分析了这些关键技术对解决问题的作用。

**关键词:** 山区; 宽带; 移动通信

## 1 引言

随着战场信息的瞬息万变,随着影响作战的要素不断增加,随着以机动性提高自身生存性的策略发展,对军事通信的宽带化、移动化要求日益增长。另外作战期间,出于战术部署要求,指挥所和作战区域还常常设置于山岳丛林地带。对于山区宽带移动战术通信如何解决,是我们面临的一个问题。

## 2 需求说明

### 2.1 应用条件

山区地形条件:丘陵或重丘,山体比高 50~300 米,并有树木(5~10 米)等植被覆盖,山体以圆椭山形为主;

使用设想:按照网管设计预案,在适当地点架设无线宽带设备,该设备即应保证进入该小区范围各终端的无线宽带移动接入,还应不依托其他通信手段完成各小区之间的中继通信。应急情况下,通过升空,解决大区域面覆盖问题。在区域网络架构开通完成的基础上,当终端节点进入此区域,就将依托区域网络,实现网内各终端节点之间的数据、话音通信。

### 2.2 传输速率、用户容量

网络分为中继线路和接入线路。中继最大传输速率不小于 4Mbps,支持点对点、点对多点直接中继转发和透明传输;传输速率不因中继次数而成几何级下降;应能支持的中继次数不小于 7 次;接入

最大传输速率不小于 1Mbps(固定或者移动:移动速度不小于 60km/h),最小传输速率不小于 256 kbps(固定或者移动:移动速度不小于 60km/h),并具有自适应速率调整,每个子网的最大接入用户数不小于 60 个。

### 2.3 业务问题

不同业务对实时性要求不同,可分为实时业务、非实时业务、附加业务。实时业务指具有时延要求的业务(不大于 1s/400 字符),需要保证资源。非实时业务指没有时延要求的业务。附加业务是在有资源时,可开展的业务。按照业务模型统计,实时业务占流量 60%,非实时业务占 30%,附加业务占 10%。

不同业务所要求的数据可达性要求不同,可分为丢失敏感业务、丢失不敏感业务丢失敏感性业务要求数据丢包率小于 2%,丢失不敏感业务要求数据丢包率小于 10%;

按照业务接入和通信状态,可分为:静止、游牧和中速移动用户。接入方式:支持随遇接入和移动接入。所有基于 IP 的业务在小区之间能无缝切换,终端网间切换时间不大于 1 分钟。

### 2.4 使用开通

按照所规定的区域,进行网管设计;按照预案架设装备,配置参数,并沿路测试和调整,方法为:前一站设备“召唤”后一站,两站之间测试正常后,前一站设备进入静默,本站转换为“召唤”,继续下站设备开通;当需要网络开通时,通过静默唤醒方式提前开通全网设备,节点唤醒时间不大于 30s;终端节点进入区域后,打开其设备,

加入网络并保持通信能力；任务结束后，逐站传递“静默”方式，全网进入静默，并根据下一任务要求，进行撤收或继续静默。

全网同时开机时，网络收敛时间小于5分钟，终端节点接入时间小于1分钟。

### 3 关键技术考虑

需求中提出的山区宽带移动通信需求，其主要问题在于：山区的地形和地貌条件严重影响了宽带无线通信系统的性能。在所有实际的部署方案中，山形、树木这些障碍物所形成的多径现象对于通信覆盖范围、传输速率形成了极大的障碍。在山区链路条件下高性能和高效地工作是我们所要解决的关键所在。

在所规定的地形条件下，要实现容量、速率、组网能力以及对业务的支撑等特定的性能要求，必须选择合适的频率、带宽、调制、双工方式、编码、均衡、纠错、分集、功率控制、扩频跳频、自适应等技术措施。下面就主要关键技术进行介绍。

#### 3.1 双工方式

中继线路采用 TDD 方式，使得中继线路可以进行上下行数据量灵活分配带宽，具有较高的资源利用率。

接入线路采用时分复用（TDMA）和冲突检测多路存取（CSMA）相结合。其中 TDMA 提供给实时对丢失敏感性业务，可采用双工和半双。CSMA 网内各个站点以竞争方式接入信道，网络中的站点在发送数据之前，先检测信道是否空闲。如果信道空闲，则开始发送数据；否则，采取一定的退避策略、重发机制发送数据包，实现数据的可靠传输，CSMA 适于提供给非实时丢失不敏感性业务。

#### 3.2 带宽调度方式

为了支持不同时延要求的业务需求，可采用的带宽调度方式也有所区别。

- 1) 实时业务，可采用 UGS 的带宽调度方式。
- 2) 非实时业务，可采用 nrtPS 的带宽调度方式。
- 3) 附加业务，可采用 BE 的带宽调度方式。

### 3.3 关键调制技术

可考虑采用正交频分复用（OFDM）调制方式。OFDM 是一种特殊的多载波通信方案，单个用户的信息流被串/并变换为多个低速码流，每个码流都用一个子载波发送。OFDM 通过快速傅立叶变换（FFT）来选用那些即便重叠也能够保持正交的波形，将宽带数据分配到并行的窄带数据流中，通过各子载波的联合编码，具有很强的抗衰落能力，有效地消除了包括频率选择性衰落等多种干扰<sup>[1]</sup>。OFDM 具有频谱利用率高、抗噪声能力强、适合高速数据传输等特点。OFDM 即充分利用信道带宽，也可以避免使用高速均衡和抗突发噪声差错。这一调制方式对于山区通信中的多径及频率选择性衰落、高带宽数据传输、复杂电磁环境中抗窄带干扰表现出优越的性能。

当然 OFDM 的载波频率偏移和相位噪声很敏感问题、高峰均功率比（PAPR）问题、频谱资源问题也应加以注意。

#### 3.4 编码技术

可以采用根据信道情况自适应改变调制及编码方式的自适应调制编解码（AMC）技术。AMC 技术是克服无线信道的时变性的一种重要链路适应技术，能够对抗信道的时变性，而且可以克服平均路径损耗、慢衰落和快衰落，对于山区通信、移动中通信都有相当的好处。它根据接收信号的质量，随时调整分组包的调制、编码方式、编码速率，使得系统在能够达到足够的可靠性的基础上，尽可能提高的数据传输速率。使用 AMC 可以使得处于信道情况好业务可以分配更高的高阶调制和少冗余纠错，从而提高平均数据吞吐量，当信道处于深衰落时，采用传输速率较低的低阶调制和大冗余纠错码进行通信，确保通信的可靠性<sup>[2]</sup>。

自适应调制编码技术保持发射功率恒定，不仅避免了功率控制技术中的“远近效应”，而且也克服了网内用户的相互干扰，降低了网络的干扰余量，解决了快速功率控制技术中的“噪声提升”效应，提高了系统的容量。

#### 3.5 纠错技术

可采用混合自动重传（HARQ）技术和低密度（LDPC）编码。

混合自动重传操作中融合了前向纠错 (FEC) 的功能, 使得每一次分组包的发送操作都能够为最终的正确解码做出贡献: 追赶合并和递增冗余。III 型 HARQ 无论是原始数据包还是重传数据包都包含原始数据信息, 仅通过对重发数据包进行解码就能够恢复出原始数据信息。灵活采用 III 型 HARQ 中单冗余版本, 可以更好地提升系统的性能。

低密度奇偶校验码 LDPC (Low Density Parity Check) 是一类可以用非常稀疏的奇偶校验矩阵定义的线性分组码, 作为一种新的纠错编码的方法, 其逼近香农限的性能、复杂度低、码本身具有很好的抗突发差错的能力。由于 LDPC 码有很好的抗衰落性, 编码增益很高, 接收机在较低的信噪比情况下仍然可以拥有较低的误码率, 可以使覆盖范围、抗多径等方面得到提升。

### 3.6 天线技术

天线技术上可以考虑多入多出天线技术和自适应天线技术。

多入多出 (MIMO) 天线技术非常适合通信范围内有阻挡的多径环境下的无线信号处理, 包括提供空间分集以及多路信道并行传输, 因其能在不增加带宽的情况下提高传输效率和频谱利用率, 因此提高了系统容量和覆盖范围。一般可以采用空时发射分集和空间复用结合模式<sup>[3]</sup>。

空时编码的主要思想是利用空间和时间上的编码实现一定的空间分集和时间分集, 从而降低信道误码率, 以对抗阻挡视距和非直视距造成的深衰落。使用空时码时, 在发端不知道信道状态信息的情况下, 系统仍能实现最大分集增益和编码增益, 但不能提高数据速率。空间复用技术是指在发射端发射相互独立的信号, 接收端采用干扰抑制 (迫零和干扰对消) 进行逐符号检测解码。空间复用虽然能最大化 MIMO 系统的平均发射速率, 但只能获

得有限的分集增益。如果将两者结合就能提供分集增益又可以提高系统容量, 从而得到高频谱效率和传输质量。

自适应天线 (AAS) 可以实现系统参数自动调整, 获得信噪比 (SNR) 增益, 减少同频干扰。自适应天线利用数字信号处理技术, 产生空间定向波束, 使天线主波束对准期望信号到达方向, 同时对干扰形成零陷, 抑制干扰, 实现期望信号的最佳接收。对于 TDD 模式下, 上行和下行共用相同的频带资源, 可以利用上 (下) 行信道的信息得到下 (上) 行信道的信息, 计算波束形成的权值。而在频分复用 (FDD) 模式下, 上行和下行的信道一般是不同的, 难以通过上 (下) 行的信息获得下 (上) 行信道信息。要想计算波束形成的权值, 需要通过反馈方式以获取信道质量信息。

### 3.7 移动IP问题

网络泛在化是未来的趋势, 基于 IP 的网络将是多种业务的公共流转平台。宽带移动网中对移动 IP 的有效管理是网络的一个重要特性。尤其是网络切换过程中的 IP 管理。移动 IP 管理中分为无线信号强度检测、强度检测判断、扫描信息传送、切换请求、切换提示、切换确认、访问切入点连接指示、访问切入点连接确认、修正请求、修正回应等过程。这需要一个完整的协议过程。

## 4 结束语

山区宽带移动通信是一个重要的问题, 同时也是一个比较困难的问题, 考虑选择合适的频率和带宽调度方式, 采用先进的调制技术、编码技术、纠错检错技术、天线技术及网络技术, 并加以合理利用, 将可能解决此问题。

### 参考文献 (略)

### 作者联系方式

通信地址: 北京海淀区小营西路 32 号院子九二炮装备研究院第四研究所

邮政编码: 100085

联系电话: 010-66345574

# 短波Lorentz信道确定性仿真模型的设计

李涛 刘德良 沈良 谢晓刚

**摘 要:** 本文根据复有色高斯噪声过程的确定性仿真模型提出了计算模型参数的方法。采用特殊值法和最小平方误差法计算模型的多普勒系数, 比较两种方法下的确定性过程概率密度函数对高斯过程理论概率密度函数的近似程度, 由仿真结果可知最小平方误差法性能优于特殊值法。采用等面积法、精确多普勒扩展法和最小平方误差法计算模型的离散多普勒频率, 比较三种方法下确定性过程自相关函数与高斯过程理论自相关函数的近似程度, 由仿真结果可知最优离散多普勒频率法性能优于其他两种方法。同时给出了确定性过程相位的计算方法。

**关键词:** 确定性仿真模型; 多普勒功率谱密度; Lorentz 分布; Rayleigh 信道

## 1 引言

短波信道中多普勒扩展通常很小, 一般在 1Hz (急剧衰落时可以达到 10Hz 以上) 左右, 如果输入的抽样信号的速率很高, 这时短波信道仿真器中的数字滤波器带宽将很窄, 从而使得滤波器的实现变得非常困难。因此通过确定性方法来模拟多普勒功率谱密度服从高斯分布或 Lorentz 分布的随机过程将是比较切实可行的方法。

设计有色高斯噪声过程的典型方法是对高斯白噪声滤波, 滤波器的冲击响应函数为信道多普勒功率谱密度的平方根。有限数量正弦曲线相加<sup>[3]</sup>的方法也得到了广泛的应用, 这个方法通过设计有限数量加权的正弦曲线近似有色高斯噪声过程。通常至少使用两个或两个以上的有色高斯噪声过程仿真无线信道模型。例如, 为了实现 Rayleigh 或 Rice 过程, 需要两个实有色高斯噪声过程; 为了实现 Suzuki (Rayleigh 和 Lognormal 过程的乘积) 过程<sup>[1]</sup>要基于三个实有色高斯噪声过程。使用  $n$  阶延迟线模型来对  $n$  条路径的频率选择性无线传播信道建模<sup>[2]</sup>, 就需要  $2n$  个实有色高斯噪声过程。

文献[1]中介绍了多种计算模型参数的方法。等距离方法和均方误差方法的特点是相临离散多普勒频率的距离相等, 其缺点 (由于等距的离散多普勒频率) 为近似的有色高斯噪声过程是周期性的。等面积方法可以对具有 Jakes 多普勒功率谱密度的随机过程的理论统计特征进行足够精度的近似, 但是对其他多普勒功率谱密度 (例如多普勒功率谱密度为高斯分布) 就不成功或要求大量的正弦曲线才能

达到足够的近似精度。Monte carlo 方法因为离散多普勒频率是随机变量, 即使正弦曲线数量很大, 设计的高斯噪声过程多普勒功率谱密度的矩也是随机变量, 与理想的矩相差很大。

但是目前的文献没有涉及短波通信中信道多普勒扩展服从 Lorentz 分布时确定性仿真模型的研究。本文采用确定性方法计算多普勒功率谱密度服从 Lorentz 分布时确定性仿真模型的参数。第二部分将讨论多普勒功率谱密度服从 Lorentz 分布的随机过程的统计性质。第三部分介绍确定性仿真模型的概念, 讨论各种不同参数计算方法并仿真比较其性能。第四部分为结论及将来工作。

## 2 Rice过程的随机解析模型

### 2.1 解析模型的描述

我们使用均值不为零的复高斯过程的绝对值定义随机过程  $\varepsilon(t)$ :

$$\mu_{\rho}(t) = \mu(t) + m(t) \quad (1)$$

$$\varepsilon(t) = |\mu_{\rho}(t)| \quad (2)$$

在公式 (1) 中, 接收信号中的散射成分用零均值的复高斯噪声过程来表示。

$$\mu(t) = \mu_1(t) + j\mu_2(t) \quad (3)$$

其中  $\mu_1(t)$ 、 $\mu_2(t)$  为实数; 方差  $Var\{\mu(t)\} = 2Var\{\mu_i(t)\} = 2\sigma_o^2$ 。短波通信中一般没有主径分量, 故  $m(t) = 0$ 。

短波衰落信道中复高斯噪声过程  $\mu(t)$  的多普

勒功率谱密度  $s_{\mu\mu}(f)$  服从 Gauss 和 Lorentz 分布。

本文研究短波通信中信道多普勒扩展服从 Lorentz 分布时如何计算确定性仿真模型的参数，功率谱密度表达式为：

$$s_{\mu\mu}(f) = \frac{2\sigma_o^2}{\pi} \frac{f_c}{(f - f_s)^2 + f_c^2} \quad (4)$$

$f_s$  是频移， $f_c$  是 3dB 截止频率， $\psi_o$  表示 Gauss 过程  $\mu_i(t)$  的平均功率， $\psi_o = \sigma_o^2$ ，即  $\psi_o = r_{\mu_i\mu_i}(0) = r_{\mu\mu}(0)/2$   $i=1,2$ 。

相应的自相关函数为：

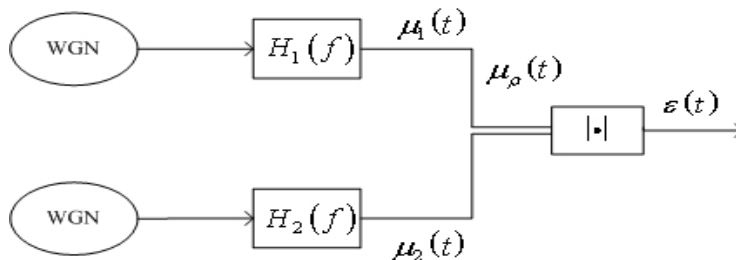


图1 Rayleigh 随机过程的解析模型

## 2.2 解析模型的统计特性

由于复高斯过程  $\mu(t)$  的多普勒功率谱密度  $s_{\mu\mu}(f)$  对 Rayleigh 过程  $\varepsilon(t)$  的幅度概率密度函数  $p_\varepsilon(x)$  和相位概率密度函数  $p_\theta(\theta)$  的性质没有任何影响[3]。由文献[3][5]可得短波信道中  $s_{\mu\mu}(f)$  为 Lorentz 分布时 Rayleigh 过程的概率密度函数  $p_\varepsilon(x)$ 、 $p_\theta(\theta)$  与 Jakes、Gauss 分布时相同。

$$p_\varepsilon(x) = \begin{cases} \frac{x}{\psi_o} e^{-\frac{x^2}{2\psi_o}}, & x \geq 0 \\ 0, & x < 0 \end{cases} \quad (7)$$

$$p_\theta(\theta) = \frac{1}{2\pi}, \theta \in [0, 2\pi) \quad (8)$$

## 3 Rice过程的确定性仿真模型

本节介绍计算仿真模型系数和参数的方法。首先定义两个实函数  $\tilde{\mu}_1(t)$ 、 $\tilde{\mu}_2(t)$ ，

$$\tilde{\mu}_i(t) = \sum_{n=1}^{N_i} \tilde{\mu}_{i,n} = \sum_{n=1}^{N_i} c_{i,n} \cos(2\pi f_{i,n}t + \theta_{i,n}) \quad i=1,2 \quad (9)$$

$$r_{\mu\mu}(t) = 2\sigma_o^2 e^{-2\pi f_c|t|} e^{j2\pi f_s t} \quad (5)$$

同时

$$r_{\mu\mu}(t) = 2 \left[ r_{\mu_1\mu_1}(t) + j r_{\mu_1\mu_2}(t) \right] \quad (6)$$

若  $f_s \neq 0$ ，自相关函数是复数，Gauss 过程  $\mu_1(t)$ 、 $\mu_2(t)$  是相关的。本文介绍  $f_s = 0$  的情况。图1表示没有频偏的（ $f_s = 0$ ）、功率谱密度服从 Lorentz 分布的 Rayleigh 过程  $\varepsilon(t)$  的解析模型的结构。

参数  $c_{i,n}$ 、 $f_{i,n}$ 、 $\theta_{i,n}$  分别称为多普勒系数、离散多普勒频率、多普勒相位。在仿真设置阶段仿真模型参数  $c_{i,n}$ 、 $f_{i,n}$ 、 $\theta_{i,n}$  都要计算出，在整个仿真运行阶段都是常数。由于所有的参数都是已知量， $\tilde{\mu}_i(t)$  在所有时间都是确定的，因此  $\tilde{\mu}_i(t)$  是确定性函数。我们可以通过如下方法定义相应的自相关函数

$$\tilde{r}_{\mu_i\mu_i}(t) = \lim_{T_o \rightarrow \infty} \frac{1}{2T_o} \int_{-T_o}^{T_o} \tilde{\mu}_i(t) \tilde{\mu}_i(t+\tau) d\tau \quad (10)$$

将(9)式代入(10)式，进行傅立叶变换，得到了自相关函数  $\tilde{r}_{\mu_i\mu_i}(t)$  和功率谱密度  $\tilde{s}_{\mu_i\mu_i}(f)$

$$\tilde{r}_{\mu_i\mu_i}(t) = \sum_{n=1}^{N_i} \frac{c_{i,n}^2}{2} \cos(2\pi f_{i,n}t) \quad (11a)$$

$$\tilde{s}_{\mu_i\mu_i}(f) = \sum_{n=1}^{N_i} \frac{c_{i,n}^2}{4} [\delta(f - f_{i,n}) + \delta(f + f_{i,n})] \quad (11b)$$

图2展示了用连续时间形式表示的 Rayleigh 过程确定性仿真模型的通用结构，可以看到需要仿真两个实有色高斯噪声过程。

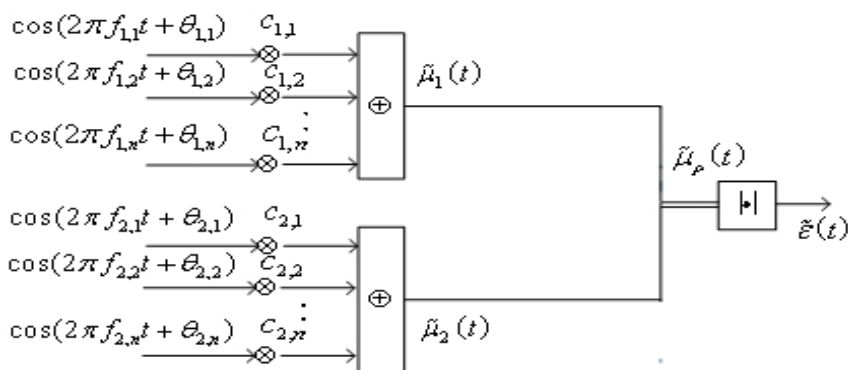


图2 Rayleigh 随机过程的确定性仿真模型

### 3.1 多普勒系数的确定

文献[3]证明了确定性过程  $\tilde{\mu}_i(t)$  趋向于均值为 0，方差为  $\sigma_o^2$  的高斯随机过程  $\mu_i(t)$ ，即

$$\lim_{N_i \rightarrow \infty} \tilde{p}_{\mu_i}(x) = p_{\mu_i}(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma_o^2}} \quad (12)$$

本文采用以下两种方法计算多普勒系数：

#### (1) 特殊值方法

仿真模型中的单条正弦曲线系数为  $c_{i,n}$ ，假设单条正弦曲线的平均功率相等，那么确定性过程  $\tilde{\mu}_i(t)$  的平均功率为：

$$\frac{c_{i,n}^2}{2} N_i = \sigma_o^2 \quad (13)$$

那么

$$c_{i,n} = \sigma_o \sqrt{2/N_i} \quad (14)$$

由文献[3]知确定性过程  $\tilde{\mu}_i(x)$  的概率密度函数为：

$$\tilde{p}_{\mu_i}(x) = 2 \int_0^\infty \left[ \prod_{n=1}^{N_i} J_0(2\pi c_{i,n} v) \right] \cdot \cos(2\pi v x) dv \quad (15)$$

其中  $J_0(\square)$  表示第一类零阶 Bessel 函数。

分别采用 5 条 ( $N_i=5$ )、7 条 ( $N_i=7$ ) 正弦曲线近似高斯过程  $\mu_i(t)$ ， $\sigma_o^2=1$ 。将由 (14) 式求得的系数  $c_{i,n}$  代入 (15) 式，可得到近似概率密度函数  $\tilde{p}_{\mu_i}(x)$ ，图 3 (a) 表示确定性过程  $\tilde{\mu}_i(t)$  的概率密度函数  $\tilde{p}_{\mu_i}(x)$  与随机过程  $\mu_i(t)$  的高斯概率密度函数  $p_{\mu_i}(x)$  的比较。

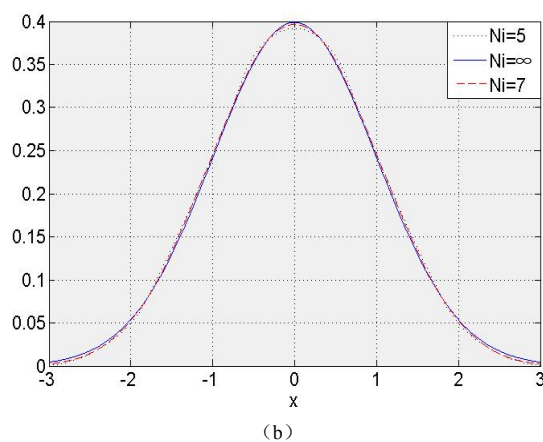
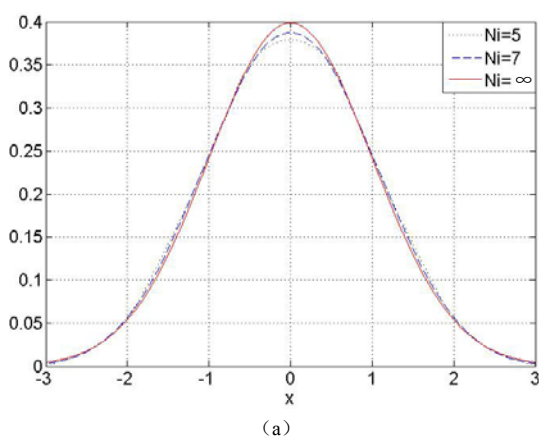


图3 近似高斯概率密度函数

#### (2) 最小平方误差法

将 (12) (15) 式代入 (16) 式，以 (14) 式中的  $c_{i,n}$  为初始值，通过搜索  $c_{i,n}$  的最优值从而求

得  $E_{p_{\mu_i}}^{(2)}$  的最小值，即通过使  $E_{p_{\mu_i}}^{(2)}$  最小化得到最优多普勒系数  $c_{i,n}^{(opt)}$ 。

$$E_{p_{\mu_i}}^{(2)} := \left\{ \int_{-\infty}^{\infty} |p_{\mu_i}(x) - \tilde{p}_{\mu_i}(x)|^2 dx \right\}^{1/2} \quad (16)$$

分别采用 5 条 ( $N_i=5$ )、7 条 ( $N_i=7$ ) 正弦曲线近似高斯过程  $\mu_i(t)$ ,  $\sigma_o^2=1$ 。将由 (16) 式求得的系数  $c_{i,n}$  代入 (15) 式, 可得到近似概率密度函数  $\tilde{p}_{\mu_i}(x)$ , 图 3 (b) 表示求得的确定性过程  $\tilde{\mu}_i(t)$  的概率密度函数  $\tilde{p}_{\mu_i}(x)$  与随机过程  $\mu_i(t)$  的高斯概率密度函数  $p_{\mu_i}(x)$  的比较。

根据以下准则衡量多普勒系数的精确性: 确定性过程  $\tilde{\mu}_i(t)$  的概率密度函数  $\tilde{p}_{\mu_i}(x)$  是否是随机过程  $\mu_i(t)$  的高斯概率密度函数  $p_{\mu_i}(x)$  的最佳近似。

比较图 3 (a)、(b) 可知最小平方误差法求得的多普勒系数集合  $\{c_{i,n}\}$  使得仿真系统的概率密

度函数  $\tilde{p}_{\mu_i}(x)$  更好地逼近理想高斯概率密度函数  $p_{\mu_i}(x)$ 。

将上述两种方法求出的系数分别代入 (16) 式, 得到各自的平方误差, 结果如图 (4) 所示。当  $N_i \geq 7$  时, 比较两种系数下的误差  $E_{p_{\mu_i}}^{(2)}$ , 其差距可以忽略。故多普勒系数可由下式确定:

$$c_{i,n} = \sigma_o \sqrt{2/N_i}, \quad \text{if } N_i \geq 7 \quad n=1, 2, \dots, N_i \quad (17)$$

显然此计算方法适用于多普勒扩展服从 Lorentz 分布的情况。

同时确定性仿真过程  $\tilde{\varepsilon}(t)$  的幅度概率密度函数  $\tilde{p}_{\varepsilon}(z)$  和相位概率密度函数  $\tilde{p}_{\nu}(\theta)$  与解析 Rayleigh 过程  $\varepsilon(t)$  的概率密度函数非常吻合<sup>[3]</sup>。

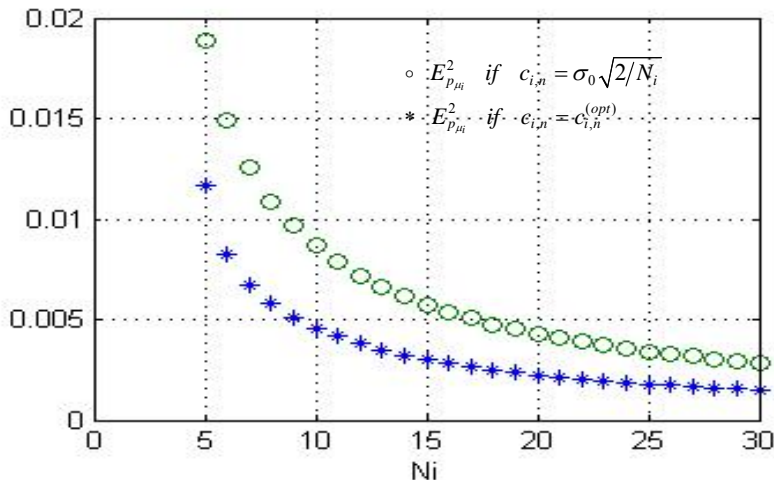


图 4 误差函数

## 3.2 确定离散多普勒频率

本文采用三种方法计算多普勒功率谱密度服从 Lorentz 分布时确定性过程的离散多普勒频率  $f_{i,n}$ 。

### 3.2.1 等面积方法

选择离散多普勒频率的集合  $\{f_{i,n}\}$ , 使得在  $f_{i,n-1} \leq f \leq f_{i,n}$  的范围内多普勒功率谱密度  $s_{\mu_i\mu_i}(f)$  (对称的) 下的面积为  $\sigma_o^2/2N_i$ ,  $n=1, 2, \dots, N_i$ ,  $f_{i,0}=0$ 。将这种方法应用于 Lorentz 功率谱密度 (对称的)  $s_{\mu_i\mu_i}(f) = s_{\mu\mu}(f)/2$  ((5) 式 (6) 式) 得到离散多普勒频率。

$$f_{i,n} = f_c \tan\left(\frac{\pi n}{2N_i}\right) \quad n=1, 2, \dots, N_i; i=1, 2 \quad (18)$$

多普勒系数采用 (17) 式计算。

### 3.2.2 精确多普勒扩展方法

根据文献[3], 可知用  $n-1/2$  代替 (18) 式中的  $n$ , 就可得到精确多普勒扩展方法下的离散多普勒频率  $f_{i,n}$ :

$$f_{i,n} = f_c \tan\left[\frac{\pi(n-1/2)}{2N_i}\right] \quad n=1, 2, \dots, N_i; i=1, 2 \quad (19)$$

### 3.2.3 最小平方误差法

由 (5) 式 (6) 式得自相关函数  $r_{\mu_i\mu_i}(t)$  的表达式 ( $f_s=0$ ):



$$r_{\mu_i \mu_i}(t) = r_{\mu \mu}(t)/2 = \sigma_o^2 e^{-2\pi f_c t} \quad (20)$$

通过使确定性仿真过程  $\tilde{\mu}_i(t)$  的自相关函数  $\tilde{r}_{\mu_i \mu_i}(t)$  (由 (11a) 式给出) 最佳逼近适当时间区间内随机过程  $\mu_i(t)$  的理论自相关函数  $r_{\mu_i \mu_i}(t)$ , 即将 (11a) 式、(20) 式代入 (21) 式, 以 (19) 式中的  $f_{i,n}$  为初始值, 通过搜索  $f_{i,n}$  的最优值从而求得  $E_{r_{\mu_i \mu_i}}^{(2)}$  的最小值, 即通过使  $E_{r_{\mu_i \mu_i}}^{(2)}$  最小化得到最优离散多普勒频率  $f_{i,n}^{(opt)}$ , 多普勒系数  $c_{i,n}$  是常数 (由 (17) 式给出)。

$$E_{r_{\mu_i \mu_i}}^{(2)} := \left\{ \frac{1}{T_o} \int_0^{T_o} |r_{\mu_i \mu_i}(t) - \tilde{r}_{\mu_i \mu_i}(t)|^2 dt \right\}^{1/2} \quad (21)$$

根据文献[1][3]推导得到  $T_o$ :

$$T_o = \frac{N_i}{2\Delta_c \sigma_c} \quad (22)$$

$$\text{其中 } \sigma_c = \frac{f_c}{\sqrt{2\ln 2}}, \quad \Delta_c = \sqrt{2\ln 2} \tan\left(\frac{\pi}{2}\right).$$

将上述三种方法求出的离散多普勒频率分别

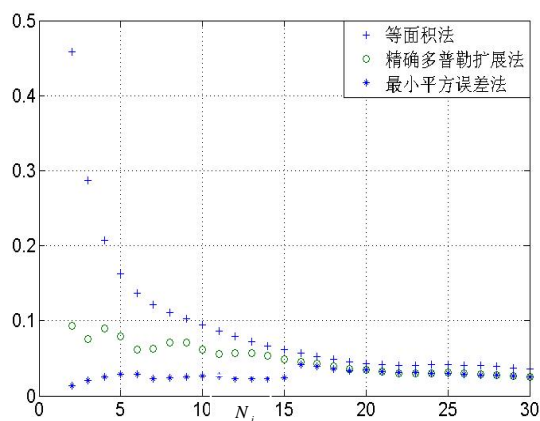


图5 误差函数  $E_{r_{\mu_i \mu_i}}^2$

从图 (5) (6) 中我们可知在 Lorentz 功率谱密度时, 最小平方误差法比另外两种方法近似误差更小、在有意义的时间区间  $[0, 2]$  内更逼近理想自相关函数。因此在 Lorentz 功率谱密度情况下我们选择最小平方误差法。

### 3.3 确定多普勒相位

多普勒相位  $\theta_{i,n}$  是均匀分布的随机变量, 只需在区间  $(0, 2\pi]$  均匀分布的随机产生器即可得到。在确定性仿真模型中本文采用确定性方法计算相

带入 (21) 式, 得到各自的平方误差  $E_{r_{\mu_i \mu_i}}^{(2)}$ ,

结果如图 (5) 所示, 仿真时  $f_c = 0.04896$ ,  $\tan\left(\frac{\pi}{2}\right) \approx 63.6567$ 。

根据以下准则衡量离散多普勒频率的精确性: 确定性过程  $\tilde{\mu}_i(t)$  的自相关函数  $\tilde{r}_{\mu_i \mu_i}(t)$  是有色高斯随机过程  $\mu_i(t)$  的理论自相关函数  $r_{\mu_i \mu_i}(t)$  的最佳近似, 即平方误差  $E_{r_{\mu_i \mu_i}}^{(2)}$  最小。

计算出离散多普勒频率  $f_{i,n}$  和多普勒系数  $c_{i,n}$  后, 利用 (11a) 式就可计算出仿真模型的自相关函数  $\tilde{r}_{\mu_i \mu_i}(t)$ 。图 (6) 展示了应用  $L_2$  规范、等面积、最小平方误差三种方法计算 Lorentz 功率谱密度时确定性过程的自相关函数。

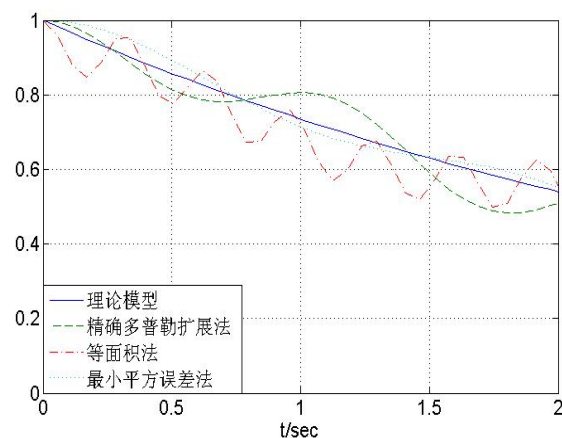


图6 近似自相关函数

位, 将标准相位向量  $\tilde{\Theta}_i$  排列就可得到多普勒相位向量  $\tilde{\theta}_i$  [3],

$$\tilde{\Theta}_i = (2\pi \frac{1}{N_i + 1}, 2\pi \frac{2}{N_i + 1}, \dots, 2\pi \frac{N_i}{N_i + 1}) \quad (23a)$$

$$\tilde{\theta}_i = (\theta_{i,1}, \theta_{i,2}, \dots, \theta_{i,N_i}) \quad i=1,2 \quad (23b)$$

多普勒相位向量  $\tilde{\theta}_i$  的分量与标准相位向量  $\tilde{\Theta}_i$  的分量相同,  $\tilde{\Theta}_i$  可以构建  $N_i!$  个不同的多普勒相位向量  $\tilde{\theta}_i$ 。对于同一个多普勒系数  $\{c_{i,n}\}$  和离散多普勒频率  $\{f_{i,n}\}$  集合, 可以构建  $N_i!$  个不同的多普

勒相位集合  $\{\theta_{i,n}\}$ ，从而构建  $N_1 \square N_2!$  个不同的复确定性过程  $\tilde{\mu}(t) = \tilde{\mu}_1(t) + j\tilde{\mu}_2(t)$ （有不同的时间性质，但可具有相同的统计性质）。

## 4 结论

本文分析了信道多普勒扩展服从 Lorentz 分布时的确定性仿真模型参数的计算方法。采用特殊值法和最小平方误差法计算模型的多普勒系数，通过仿真可知最小平方误差法性能优于特殊值法。采用

等面积法、精确多普勒扩展法和最小平方误差法计算模型的离散多普勒频率，通过仿真可知最小平方误差法性能优于其他两种方法。同时给出了确定性过程相位的计算方法，从而得到了短波信道确定性仿真模型的参数。文中所述方法可应用于短波信道仿真器的设计，有较大的理论意义和工程应用前景。文中重点研究了如何计算仿真模型参数，下一步将重点关注仿真模型的高阶统计性质，如电平交叉率、平均衰落时间和衰落间隔的概率密度函数。

## 参考文献

- [1] M. Patzold, U. Killat, and F. Laue, "A deterministic digital simulation model for Suzuki processes with application to a shadowed Rayleigh land mobile radio channel," IEEE Trans. Veh. Technol., vol. 45, no. 2, pp. 318–331, 1996.
- [2] John G. Proakis. Digital Communication, 4th ed. 北京: 电子工业出版社, 2006.
- [3] M. Patzold, U. Killat, F. Laue, and Y. Li, "On the statistical properties of deterministic simulation models for mobile fading channels," IEEE Trans. Veh. Technol., vol. 47, no. 1, pp. 254–269, 1998.
- [4] P. Hoher, "A statistical discrete-time model for the WSSUS multipath channel," IEEE Trans. Veh. Technol., vol. VT-41, no. 4, pp. 461–468, Nov. 1992.
- [5] A. Papoulis, *Probabilities, Random Variables, and Stochastic Processes*, 3rd ed. New York: McGraw-Hill, 1991.
- [6] Theodore S. Rappaport, *Wireless Communication Principles and Practice*, 2nd ed. 北京: 电子工业出版社, 2004.
- [7] M. Patzold, U. Killat, Y. Shi, and F. Laue, "A deterministic method for the derivation of a discrete WSSUS multipath fading channel model," European Trans. Telecommun. (En), submitted and accepted for publication.

## 作者联系方式

通信地址: 南京市标营 2 号解放军理工大学通信工程学院移动教研室

邮政编码: 210007

联系电话: 13218003702      025-80828495

# 应用启发式算法解决多星遥感任务规划问题

李湘 陈健 靳峰 朱博

**摘要:** 本文根据多星遥感任务规划的特点, 提出了启发式算法在解决多星遥感任务规划问题中的应用。文章从任务规划模型描述、启发式算法求解框架、启发式算法的变量设计、启发式规则的构造几方面进行研究, 并通过实验数据进行比较, 分析了不同启发式规则在遥感任务规划中的适应性, 对于遥感任务规划技术的研究具有参考价值。

**关键词:** 近似算法; 遥感任务规划; 启发式算法; 启发式规则

## 1 前言

卫星遥感在国民生产、生活和国家经济、政治、军事领域的应用越来越广泛, 如何利用有限的卫星资源、地面接收站资源高质量完成尽可能多的遥感任务, 是遥感卫星综合任务规划要解决的问题。

从国内外研究资料而看, 即便是最简单的单星任务规划模型, 其求解都是 NP-Complete 问题。而多星遥感任务规划更加复杂, 由于问题的难解性, 所以象规划问题的割平面算法、拉格朗日松弛算法、分支定界算法等在一般情况下将需要指数函数的运行时间。为了在一定的时间、空间范围内求解这些问题, 避免问题求解过程中状态信息的组合爆炸, 对该问题的研究多采用近似算法。

现代启发式算法是基于生物学、物理学和人工智能的一类近似算法, 具有全局优化性能、鲁棒性强、通用性强且适于并行处理的特点, 它比较接近于人类的思维方式, 易于理解, 用这类算法求解组合优化问题在得到最优解的同时也可以得到一些次优解, 便于规划人员研究比较。

## 2 问题描述

多星遥感任务规划是一个非常复杂的问题, 需要考虑的因素错综复杂, 包括卫星载荷的多种约束、任务优先级、地面接收站的属性、问题规模等。其中卫星载荷约束尤其复杂, 主要包括:

- 1) 卫星的数据存储容量;
- 2) 卫星数据下传与数据存储的速率比;

- 3) 卫星单个圈次最大侧视调整次数;
- 4) 卫星单个圈次最大开机时间;
- 5) 卫星每个圈次的运行时间;
- 6) 卫星侧视校准时间;
- 7) 卫星侧视调整速率;
- 8) 卫星最短开机时间。

在多星遥感任务规划问题中, 问题规模至关重要, 不同的规模常常会导致算法性能差异很大, 问题规模主要由下列因素决定:

- 1) 遥感任务的数目;
- 2) 卫星数目;
- 3) 地面数据接收站的数目;
- 4) 调度有效期的时间长度;

多星遥感任务规划就是要在一定的时间周期内, 合理安排既定的卫星资源和地面数据接收资源, 尽早完成尽可能多的遥感任务, 获得对资源的最佳利用。

## 3 启发式算法设计

根据多星遥感任务规划特点, 我们设计了遥感任务需求度和时间窗口争用度作为该问题的变量排序启发式和变量值启发式。

遥感任务需求度

$$Req = \frac{w}{\sum_n \frac{e_i - b_i}{d_i}}$$

其中  $w$  是当前任务的优先级,  $n$  是该任务可用时间窗口的数目,  $e_i, b_i$  和  $d_i$  分别是时间窗口  $i (1 \leq i \leq n)$  的开始时间, 结束时间和该任务在窗

口执行时的持续时间。由于本问题所考察的卫星有些具有沿星下点方向的俯仰能力，所以通常情况下，会有  $d_i \leq e_i - b_i$ ，使得最终解不仅要指定任务的执行时间窗口，还要给出任务在时间窗口中的开始时刻。

如果仅仅按照遥感任务的优先级来选取下一个要调度的任务，对于优先级相差不大，可用时间窗口的数目和长度却相差很多的两个任务来说有失偏颇。式中的分母部分刻画了该任务在其可用时间窗口中的随意度累积效果。对于任务的每个时间窗口来说，任务的开始时刻可以安排在  $[b_i, e_i - d_i]$  之间的任意时刻。例如图 1 中所示，任务 1 虽然优先级较高，但是该任务有两个可用时间窗口，且每个时间窗口的长度都要远大于该任务在该窗口内的持续时间，即剩余的观测机会多；任务 2 尽管优先级较低，但其可用时间窗口的个数和在该窗口内执行时间的可选择性较差，即剩余的观测机会少。如果仅仅考虑任务的优先级，某些优先级低且剩余观测机会少的任务就很难得到本就紧缺的观测机会。所以当选择下一个要调度的任务时，不能简单地以任务优先级作为唯一的衡量标准，综合考虑任务的优先级和任务的剩余观测机会两个因素会更全面和更恰当。

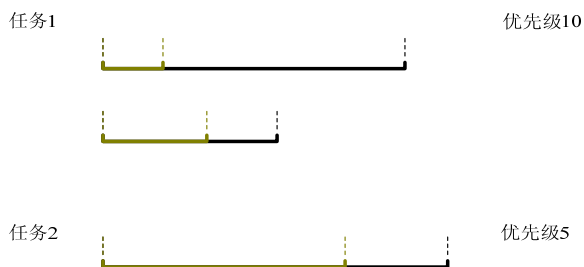


图 1 任务的实际执行时间和任务的可用时间窗口之间的关系

每调度一个任务之前，都会对所有未调度的任务进行按遥感任务需求度为指标的排序，任务需求度高的优先调度。这种调度任务的策略可以将优先级高且剩余观测机会少的“更饥渴”任务优先调度，一定程度上提高了构造可行解的效率。

时间窗口争用度

$$Con = \sum_m \frac{s_{ij}}{d_{ij}} \times w_i$$

其中  $m$  是未调度任务的个数， $w_i$  是未调度任务  $i$  ( $1 \leq i \leq m$ ) 的优先级， $d_{ij}$  是安排当前时间窗口会

对未调度任务的某个时间窗口  $j$  产生影响时，窗口  $j$  的持续时间， $s_{ij}$  是产生影响的长度。产生影响是指当前窗口和某个未调度任务的时间窗口  $j$  的卫星资源相同时，两个时间窗口之间的时间重合量。如图 2 所示。

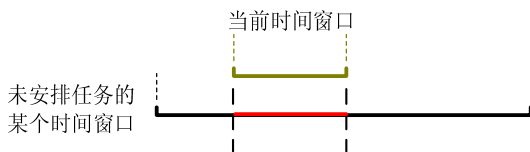


图 2 当前时间窗口对未安排任务的影响

图中点线（虚线）部分是当前需要计算窗口争用度的时间窗口，黑色部分是未安排任务的某个时间窗口，需要注意的是该时间窗口必须与当前窗口由同一个卫星执行时才有窗口争用的概念。当满足了这个前提之后，如果两个时间窗口在时间范围上有重叠，图 4 中粗线（红色）部分为重叠部分，则重叠部分的长度代表了当前窗口对应任务与未调度任务之间在时间上的争用程度。对这个程度在所有未调度任务范围内进行累积，就能够衡量遥感任务选用当前时间窗口的争用程度。

如果某个时间窗口的争用度高，则表明该时间窗口被很多未调度任务所争用，在给选定任务安排时间窗口时，应该安排在争用程度低的时间窗口，这种策略有利于我们更多地安排遥感任务，也有利于我们更快的生成可行解，还有利于避免出现不同卫星之间任务负荷不均衡的情况。

## 4 三种启发式规则构造

为了构造三种启发式规则，我们首先做如下符号定义。

所有遥感任务的集合  $T$ ，未安排遥感任务的集合  $U$ ，无法安排遥感任务的集合  $C$ ；

已安排的遥感任务集合  $S$ ， $\forall s \in S$ ，完成该任务  $s$  的卫星  $sat_s$ ，任务的持续时间  $d_s$ ，任务的开始时间  $b_s$ ，结束时间  $e_s$ ，侧视角度  $a_s$ ；

当前调度任务  $u_c$ ，当前调度任务的当前时间窗口  $tw_c$ ；

所有卫星集合  $SAT$ ， $\forall sat \in SAT$ ，每个卫星的已安排任务集合  $S_{sat}$ ；

$\forall u \in U$ ，任务的优先级  $w_u$ ，任务需求度

$Req_u$ , 可用时间窗口集合  $TW_u$ ,  $\forall tw \in TW_u$ , 任务的持续时间  $d_{tw}$ , 完成该时间窗口的卫星  $sat_{tw}$ , 窗口的开始时间  $b_{tw}$ , 窗口的结束时间  $e_{tw}$ , 窗口的侧视角度  $a_{tw}$ , 窗口争用度  $Con_{tw}$ 。对于可用时间窗口, 窗口的持续时间不小于任务的持续时间是其必要条件。

### (1) 先到先服务

先到先服务规则以服务对象到达服务系统的时间先后顺序来安排对象被服务的次序。在研究中, 将卫星系统作为服务系统, 将遥感任务作为服务对象, 以遥感任务的最早可用时间窗口的开始时刻作为该对象到达服务系统的时刻。先到先服务规则的调度流程如下。

步骤 1:  $S = \Phi, U = T, C = \Phi, \forall sat \in SAT, S_{sat} = \Phi$ ;

步骤 2: 如果  $U = \Phi$ , 则算法终止; 否则转到步骤 3;

步骤 3:  $\forall u \in U$ , 检查  $TW_u$ , 确保  $\forall tw \in TW_u, e_{tw} - b_{tw} \geq d_{tw}$ ;

如果  $tw_0$  不满足以上条件, 则将  $tw_0$  从  $TW_u$  中删除;

如果  $TW_u = \Phi$ , 则  $U \leftarrow U - u, C \leftarrow C + u$ , 转到步骤 1;

否则对  $TW_u$  中的元素按照时间序升序排列;

步骤 4:  $b_{tw_{u0}} = \min_U \min_{tw} (b_{tw_u}), u_c \leftarrow u_0, tw_c \leftarrow TW_{u_c}$  中开始时间最早的时间窗口;

步骤 5: 将  $tw_c$  分解为  $tw_{c1}$  和  $tw_{c2}$ , 同时  $TW_{u_c} \leftarrow TW_{u_c} - tw_c + tw_{c1} + tw_{c2}$ ;

$tw_{c1}$  的开始时间和结束时间分别为  $b_{tw_c}$  和  $b_{tw_c} + d_{tw_c}$ ;

$tw_{c2}$  的开始时间和结束时间分别为  $b_{tw_c} + d_{tw_c}$  和  $e_{tw_c}$ ; 并且  $tw_c \leftarrow tw_{c1}$ ;

步骤 6: 按照以下顺序对  $tw_c$  进行一系列约束满足可行性检查:

所有已调度任务的时间一致性约束  $\rightarrow u_c$  是否满足相关卫星的单圈最大开机时间约束  $\rightarrow u_c$  是否满足相关卫星的存储容量约束  $\rightarrow u_c$  是否满足与其前驱任务和后继任务之间的侧视调整时间约束  $\rightarrow u_c$  是否满足相关卫星的单圈最大侧视调整次数约束;

如果以上任一约束未能满足, 则将  $tw_c$  从

$TW_{u_c}$  中删除, 并转到步骤 1, 否则转到步骤 6;

步骤 7:  $U \leftarrow U - u, S \leftarrow S + u, S_{sat_u} \leftarrow S_{sat_u} + u$ ;

如果  $\exists u_0 \in U, s.t. (sat_{tw_{u_0}} = sat_{tw_c}) \cap (tw_{u_0} \text{ overlap with } tw_c)$ , 则对  $tw_{u_0}$  的可用时间信息进行修改, 并转到步骤 1。

### (2) 简单优先级

简单优先级的思想是按照任务的优先级来选取任务, 任务选定以后, 任务执行时间窗口的选择遵循时间靠前的窗口优先的原则。简单优先级规则的调度流程与先到先服务规则的调度流程相同。

### (3) 高级优先级

高级优先级跟简单优先级相同之处在于也是先选定下一个要调度的任务, 之后再对该任务安排时间窗口。不同点在于, 任务的选择顺序按照遥感任务需求度降序安排, 窗口的选择按照时间窗口争用度升序安排。这样, 高级优先级规则不但综合了窗口的时间信息和任务优先级信息, 同时兼顾了每个未调度任务的可用时间窗口的长度, 考虑了当前任务可能执行时间窗口与其他未安排任务的可用时间窗口之间的争用程度, 从而使调度过程具有一定的前瞻性, 避免赋值失败, 更智能更高效地生成完整解。高级优先级规则的调度流程如下:

步骤 1:  $S = \Phi, U = T, C = \Phi, \forall sat \in SAT, S_{sat} = \Phi$ ;

步骤 2: 如果  $U = \Phi$ , 则算法终止; 否则转到步骤 2;

步骤 3:  $\forall u \in U$ , 检查  $TW_u$ , 确保  $\forall tw \in TW_u, e_{tw} - b_{tw} \geq d_{tw}$ ;

如果  $tw_0$  不满足以上条件, 则将  $tw_0$  从  $TW_u$  中删除;

如果  $TW_u = \Phi$ , 则  $U \leftarrow U - u, C \leftarrow C + u$ , 并转到步骤 1;

否则对  $TW_u$  中的元素按照时间序升序排列;

步骤 4:  $Req_{u_0} = \max_{u \in U} (Req_u), u_c \leftarrow u_0$ ;

步骤 5:  $\forall tw \in TW_{u_c}$ , 按照  $\Delta t$  的时间间隔对  $tw$  进行分解, 并对  $TW_{u_c}$  进行更新;

$Con_{tw_0} = \min_{TW_{u_c}} (Con_{tw}), tw_c \leftarrow tw_0$

步骤 6: 按照以下顺序对  $tw_c$  进行一系列约束满足可行性检查 (约束同“先到先服务”中的步骤 6 的约束):

如果任一约束未能满足, 则将  $tw_c$  从  $TW_{u_c}$  中删除, 并转到步骤 1, 否则转到步骤 6;

步骤 7、 $U \leftarrow U - u, S \leftarrow S + u, S_{sat_u} \leftarrow S_{sat_u} + u$  ;  
如果  $\exists u_0 \in U, s.t. (sat_{tw_{u_0}} = sat_{tw_c}) \cap (tw_{u_0} \text{ overlap with } tw_c)$   
则对  $tw_{u_0}$  的可用时间信息进行修改, 并转到步骤 1。

5 启发式求解框架

根据多星遥感任务规划要求和启发式算法的特点, 本文设计多卫星遥感任务规划的启发式算法求解框架如图 3 所示。

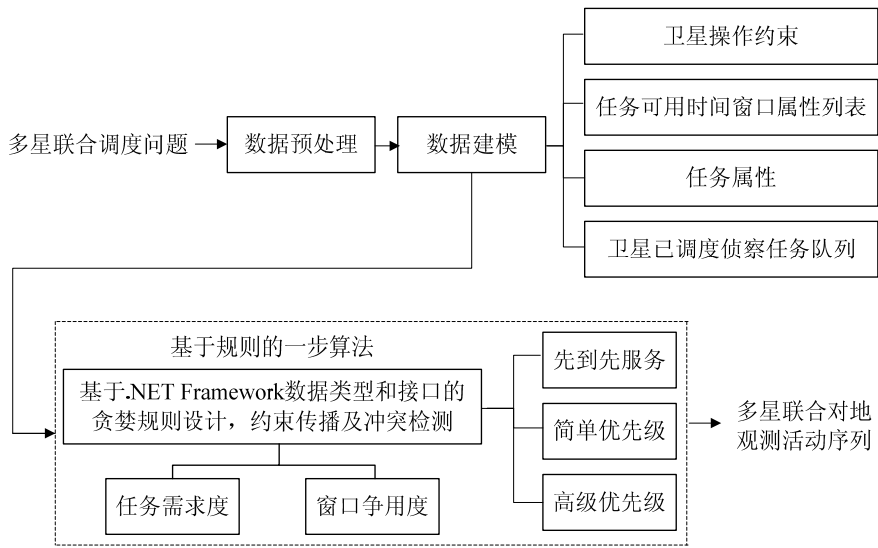


图 3 多卫星遥感那任务规划的启发式算法求解框架

从图中可见问题的求解思路。经过数据预处理过程, 选择合理的数据结构对数据进行建模。然后结合问题结构, 在定义算法中的变量选择启发式(任务需求度)和变量值启发式(窗口争用度)的基础上, 设计三种启发式规则。

6 启发式算法性能

6.1 测试数据生成

为了检测启发式算法在解决多星遥感任务规划问题中的性能, 本文根据多星遥感任务规划问题的基本结构特征, 设计了一定的算例。这些算例针对性强, 可调参数又允许系统地控制和改变问题的具体特性, 以便修正数据的偏颇性。

具体在生成的时候, 随机算例主要考虑了两种类型的可调控制参数。第一类是与问题复杂程度相关的参数, 主要包括问题规模相关参数和任务优先级参数。

第二类是与问题的具体结构特点相关的参数, 主要包括卫星有效载荷约束和地面站属性。

为了简化问题, 同时也是从问题的一般性或当

前的实际情况出发, 在生成随机测试算例时, 没有包括对可能存在的一些更复杂的实际约束的考虑。更明确地说, 随机数据在生成时采用了如下的一些假设。

- 1) 所有实例中调度的开始时间都设为 0;
- 2) 可供使用的卫星及其轨道特征从 STK 提供的近地极轨卫星想定数据中随机抽取。
- 3) 地面目标均为点目标, 每个点目标的地理位置在北纬 20 度 北纬 50 度, 东经 70 度 东经 130 度之间(即中国陆上领土范围内)随机生成;
- 4) 每个点目标的优先级在 0 到用户指定最大优先级之间随机生成;
- 5) 可供使用的地面站及其地理位置从 STK 提供的中国境内的地面站想定数据中随机抽取;

按照上述方式生成的数据, 还要经过预处理过程以后, 才是真正对算法产生实际影响的数据。预处理可以将随机数据中的一些无效或不合理特征剔除, 避免对算法的性能评价造成干扰。从而使得上述方式生成的模拟数据在保持问题的基本结构特征的基础上, 扩展了数据的随机性, 方便了对算法稳定性的评估。

6.2 算例的大规模计算分析

针对生成的不同规模的测试数据，表 1 给出不

同启发式规则之间的计算性能比较。表中问题实例的命名规则是：TestSets n-m-p 代表测试数据集的规模是 n 个遥感任务，m 个卫星，p 个调度周期。

表 1 不同启发式规则之间的计算结果比较

问题实例	先到先服务规则		简单优先级规则		高级优先级规则	
	未完成任务总价值	CPU 时间（秒）	未完成任务总价值	CPU 时间（秒）	未完成任务总价值	CPU 时间（秒）
TestSets100-2-2	20	0.3	18	0.3	0	0.4
TestSets100-2-5	400	0.5	390	0.5	373	0.7
TestSets200-5-2	908	1.1	788	1.1	8	1.1
TestSets200-5-5	460	1.3	420	1.3	8	1.4
TestSets300-5-2	8004	1.8	7204	1.8	5519	1.7
TestSets300-5-5	6100	1.6	5500	1.6	4299	1.8
TestSets400-5-2	13076	1.6	12076	1.6	10367	1.9
TestSets400-5-5	12109	1.5	11609	1.5	11067	1.9
TestSets500-5-2	19002	1.7	18202	1.8	17517	2.0
TestSets500-5-5	9076	1.8	8315	1.8	1745	2.1
TestSets800-5-2	48790	10.1	44596	10.2	36104	15.0
TestSets800-5-5	49615	10.1	45215	10.3	40615	16.0
TestSets1000-5-1	49087	15.0	44928	15.2	37500	20.2
TestSets1000-5-2	59890	16.0	57820	16.3	47566	23.5
TestSets1000-5-1	54864	18.0	52474	18.2	54122	24.6
TestSets1000-5-2	76712	17.7	73615	17.9	55191	23.1
TestSets1000-5-2	78934	16.9	75987	17.0	65400	23.3
TestSets1000-8-1	62340	18.0	59802	18.2	51368	25.0
TestSets1500-8-2	98903	30.3	96210	30.6	83654	50.0

从算例比较的结果来看，算法理论上的预期与算例的计算结果基本上是一致的。先到先服务规则的计算时间最短，但是返回解的质量较差，也不够稳定，主要原因在于先到先服务的规则没有考虑任务的优先级，仅仅考虑了窗口可用时间先后关系，在安排时间窗口时也没有对潜在的窗口时间冲突进行规避。简单优先级性能和先到先服务差不多。高级优先级规则的计算时间相比先到先服务规则略长，多出的时间耗费主要体现在对遥感任务需求度

和时间窗口争用度的计算和比较排序上，但是时间上的代价却换来了更多任务的调度，解的质量得到了一定的提高。当问题规模不大时，基于规则的算法在计算时间上，不同规则之间还是大致相当的，而当问题规模增加，任务数目达到 800 个以上时，先到先服务规则的计算时间就相比高级优先级少很多了。用户可以根据其自身时效性和算法质量的要求，选用不同的规则算法。

参考文献（略）

作者联系方式

通信地址：北京 61646 部队  
邮政编码：100085  
联系电话：13141313888

# 数据挖掘技术在军队信息化建设中的应用

李兴生 徐福明

**摘 要:** 本文以数据挖掘技术在军队信息化建设中的典型应用为重点,在介绍数据挖掘技术基本特点和功能的基础上,对军队信息化建设典型应用中的数据挖掘实现方法进行了深入探讨,并提出了相应对策。

**关键词:** 数据挖掘; 信息化; 知识发现

## 1 引言

近半个世纪以来,计算机和信息技术的高速发展给人类社会带来了巨大的变化与影响,数据成为重要的战略资源。由于技术的进步,人们能以更快速、更容易、更廉价的方式获取和储存数据,数据库应用的规模、范围和深度不断扩大,数据库被广泛用于商业管理、政府办公、科学研究和工程开发等,并且这一势头仍将持续发展下去,使得数据及其信息量以指数形式增长。在这信息爆炸的时代,信息过量几乎成为人人需要面对的问题。由于海量数据的复杂性和数据处理的时效性妨碍了人们对数据的使用,人们陷入了“数据丰富,但知识缺乏”的困境。据估计,目前一个大型企业数据库中的数据,只有 7% 得到很好的应用。在这些大量数据的背后隐藏了很多具有决策意义的信息,那么如何及时得到这些有用的知识呢?如何才能不被信息的汪洋大海所淹没,提高信息利用率呢?面对这一严峻挑战,知识发现技术应运而生,并得以蓬勃发展,越来越显示出其强大的生命力,而知识发现的核心技术就是数据挖掘。

## 2 数据挖掘的定义和基本过程

数据挖掘又被称为数据开采,就是从大量的、不完全的、有噪声的、模糊的、随机的数据中,提取隐含在其中的、人们事先不知道的、但又是潜在有用的信息和知识的过程<sup>[1]</sup>。人们把原始数据看作是形成知识的源泉,就像从矿石中采矿一样。原始数据可以是结构化的,如关系数据库中的数据,也可以是半结构化的,如文本、图形、图像数据。发

现知识的方法可以是数学的,也可以是非数学的;可以是演绎的,也可以是归纳的。发现的知识可以被用于信息管理、查询优化、决策支持、过程控制等,还可以用于数据自身的维护。因此,数据挖掘是一门广义的交叉学科,它汇聚了不同领域的研究者,尤其是数据库、人工智能、数理统计、可视化、并行计算等方面的学者和工程技术人员。数据挖掘技术从一开始就是面向应用的。它不仅是面向特定数据库的简单检索查询调用,而且要对这些数据进行微观、中观乃至宏观的统计、分析、综合和推理,以指导实际问题的求解,企图发现事件间的相互关联,甚至利用已有的数据对未来的活动进行预测。同时需要指出的是,这里所说的知识发现,不是要求发现放之四海而皆准的真理,也不是要去发现崭新的自然科学定理和纯数学公式,更不是什么机器定理证明。所有发现的知识都是相对的,是有特定前提和约束条件、面向特定领域的,同时还要能够易于被用户理解,最好能用自然语言表达发现结果。数据挖掘的研究成果是很讲求实际的。

正因为数据挖掘技术的多样性,也导致了数据挖掘系统的多样性。数据挖掘是一个多阶段的处理过程,由三个主要阶段组成:数据准备(包括数据清理和集成、数据选择、数据变换)、数据挖掘、结果的表示与解释。数据挖掘所能发现的知识有如下几种。

广义型知识:反映同类事物共同性质的知识;

特征型知识:反映事物各方面的特征知识;

差异型知识:反映不同事物之间属性差别的知识;

关联型知识:反映事物之间依赖或关联的知识;

预测型知识:根据历史的和当前的数据推测未



来数据;

偏离型知识:揭示事物偏离常规的异常现象。

所有这些知识都可以在不同的概念层次上被发现,随着概念树的提升,从微观到中观再到宏观,以满足不同用户、不同层次决策的需要。至于发现工具和方法,常用的有分类、聚类、模糊理论、神经网络、可视化、决策树、遗传算法、支持向量机、贝叶斯信任网络、不确定性推理等。

### 3 数据挖掘在军队信息化建设中的应用

建设信息化军队所涉及的军事技术多、覆盖面广、先进程度高,在通信和计算机技术日新月异和先进武器层出不穷的今天,如何有效利用已有的大量数据和信息,成为当前部队需要迫切解决的问题。军事决策者需要的是决策建议,希望及时获得军事态势信息,而不是一大堆“泥沙俱下”的杂乱信息。信息优势要转化为决策优势,就需要各种技术的支持。在专家系统和有关数学模型无法处理时,数据挖掘方法往往能发挥重要的作用。数据挖掘研究及其推广应用对于解决信息爆炸、辅助军队高层次决策,促进军队信息化建设的发展具有重大意义。数据挖掘在军队信息化建设中的应用是多方面的,不可能一一列举,此处只列举部分典型应用:

#### 3.1 目标识别

目标识别包括电磁辐射源识别和目标平台分类识别。首先利用数据挖掘的降维算法提取出对识别有用的最佳特征集合,然后在这些特征所组成的识别子空间中利用统计、神经网络和粗糙集等方法识别目标。如雷达辐射源识别中,已知目标雷达的射频、重频、脉宽等属性信息,就能依据挖掘出的特征规则对雷达型号进行识别<sup>[2]</sup>。

#### 3.2 目标定位

现代战争中导弹与反导弹的大量使用,给电磁波的辐射源及其载体的生存带来极大的威胁。因此无源定位技术,非常受军事专家们尤其是海军军事家的青睐,各国都在大力探求用纯方位传感器进行多目标定位的技术。由于算法复杂性的问题,一般

算法无法求解,而遗传算法在解决了编码和适应度函数选取的问题后,可以应用在多纯方位传感器多目标定位中。

#### 3.3 武器目标分配

可以利用粗糙集、神经网络、模糊动态规划、遗传算法等方法辅助决策武器目标分配。例如利用粗糙集理论及规划模型相结合的方法处理目标分配问题,将射击方案的效果作为决策属性,依据已有数据或作战经验,根据粗糙集约简的概念挖掘射击规则,并取总体效果为规划模型的优化目标,用定性与定量相结合的方法解决目标分配问题<sup>[1]</sup>。

#### 3.4 态势评定与威胁估计

态势评定中可以利用数据挖掘技术进行数据处理,对数据进行压缩、聚集,并生成态势关联规则,为决策人员提供帮助。另外可基于神经网络、模糊理论和贝叶斯网络等方法进行威胁等级评估,其结果能够比较准确地反映威胁源的真实威胁程度,从而减少人为因素导致的决策失误<sup>[4]</sup>。

#### 3.5 网络管理

数据挖掘技术在网络管理中也有广泛应用,例如军事通信网络告警处理。在军事通信网络的运行过程中,告警数目是相当可观的,利用数据挖掘中的关联规则挖掘技术,可挖掘出通信网络告警数据中的很多有规律、有价值的规则,有助于网络管理员根据现有情况做出合理的判断,从而进行有效管理和预测。另一个例子是利用 Web 挖掘的方法来解决网络拥挤的问题<sup>[5]</sup>。利用数据挖掘技术确定一些典型的进入模式,网站服务器就可以把一些用户可能要的东西预先发到用户的浏览器里或者是代理服务服务器上,可以显著提高用户的响应时间。

#### 3.6 指挥自动化系统效能评估

由于指挥自动化系统是一个人机交互的复杂系统,交织着许多难以理清的物质流与信息流构成的反馈控制环路,很多场合难以建立通用的数学模型来描述。但可以利用历史数据和客观事实,通过数据挖掘技术从中提取与效能有关的模式和规律,来描述效能评估过程中无法用通用数学模型描述的系统参量之间的关系。对那些既不能用解析方法建立

数学模型求解,也不能获得足够数据进行挖掘的问题,则利用专家经验和知识来解决。例如通过部队试验和系统联试,我们可以获得相关数据。利用数据挖掘和知识发现,可以获得多个指标对武器不确定半径的影响关系,如红方指挥控制能力(包括指挥容量、指挥跨度、作战计划生成时间、武器引导批数等),情报获取能力(包括获取手段、侦察范围、情报融合时延等),预警探测能力(包括探测距离、目标发现概率、预警时间等)以及通信时延等。

### 3.7 网络入侵检测

虽然军队内部的网络是独立的,但这并不能保证网络是安全的。据相关机构统计,来自系统内部的攻击行为在整个系统受到的攻击中占到了70%以上。也就是说实际上在系统资源损失中,更大一部分的威胁来自系统内部。入侵检测正是根据网络攻击行为而进行设计的,它一般不是采取预防措施以防止入侵事件的发生,而是通过对包括计算机系统及网络用户行为的监控,利用数据挖掘方法进行入侵分析,不仅能够发现已知的入侵行为,而且有能力发现未知的入侵行为,并可以通过学习和分析入侵手段,及时地调整系统策略以加强系统的安全性<sup>[6]</sup>。

### 3.8 情报处理

运用数据挖掘技术可以对情报进行智能化加工处理。在情报加工中,首先利用数据挖掘技术对采集的情报素材进行智能化自动处理,对信息进行分类、摘要、聚类等加工处理,完成情报的初步加工和过滤;然后再通过人工对信息进行加工处理,比如筛选情报、编写情报报告、生成和维护情报简报等。

### 3.9 空间数据库

在现代化战争和国防建设中,地形地貌侦察、军事目标跟踪监视、飞行器定位、导航、武器制导、打击效果侦察、战场仿真、作战指挥等方面,对空间信息的采集、处理、更新提出了极高的要求,由于数据库技术以及数据收集技术的发展,导致了具有海量数据规模的空间数据库的出现。庞大的数据量已经远远超出了人为分析解释的能力范

围,所以空间数据挖掘就成了急待研究的领域。数据挖掘可在空间数据库中发现知识,用来支持遥感解译自动化和地理信息系统空间分析的智能化。

### 3.10 装备维修

在工程装备向信息化发展的今天,工程装备的使用、维护、生产部门之间需要一个快速协同、相互沟通的信息数字平台。利用平时使用、维修过程中具体数据的记录积累,通过数据挖掘找出规律,设计、生产部门才能制定出最佳修改方案,研制出更有战斗力的装备;工程装备的维修和质量评估部门就可以确定工程装备哪些部位适于定时修理,哪些部位适于视情修理,提出和优化维修方案,达到保障有力,提高经济效益;领导机关才能准确掌握各装备的故障规律,为制定符合实际需要的备件储备计划提供科学可靠的依据。

### 3.11 图像处理

利用数据挖掘方法可以进行图像识别和图像恢复的处理。在复杂的战场环境中,由于成像系统的不完善、传输介质的影响以及成像系统与被摄景物的相对运动等因素,使得摄取的图像存在程度不同的失真,利用遗传算法或遗传算法与贝叶斯方法相结合的方法可以得到较好的图像恢复效果。在战场图像识别中,噪声是一个不可忽视的因素,获得的侦察图像均是低信噪比的,利用遗传算法可以较好地完成任务。

## 4 为实施数据挖掘应采取的措施

为有效实施数据挖掘,应完善以下措施。

### 4.1 建立和完善的各种应用数据库

为了支持做出决策,必须注重数据的收集和管理,维持一些大的数据库,数据库应包括敌方的作战能力、己方军队的作战能力、导弹的命中率、战略情报、敌军和我军的行动原则、地形图和航路图等。并通过健全规章制度,保持数据的连续性、持续性和实效性。

## 4.2 注重可视化用户界面的开发

可视化用户界面可以帮助用户与数据挖掘系统进行交流。一方面用户可以通过它将自己的挖掘任务提交给挖掘系统,另一方面它可以向用户展示数据挖掘的结果。

## 4.3 注重人员业务素质的培养

要想真正做好数据挖掘,需要对业务的深入了解和数据分析经验。要结合自己的本职工作,在自己熟悉的领域探索数据挖掘的应用,这样才能较好地进行人机交互,才能对挖掘出的信息去伪存真,真正找到有用的知识。

## 4.4 遵守数据驱动、需求牵引的原则

没有一种数据挖掘算法是万能的。不同的问题,需要用不同的方法去解决。即使对于同一个问题,可能有多种算法,这个时候,也需要评估对于这一特定问题和特定数据哪一种算法表现好。

## 4.5 注重数据挖掘的安全性和保密性

当从不同角度和不同抽象层次观察数据的时候,常常会涉及敏感信息,这就要考虑所挖掘信息的安全性和保密性,这需要制定相应的保密规定和严格的操作规范。

## 5 结束语

数据挖掘技术可应用于军队信息化建设的方方面面,是实现数据向知识转化的关键。需要强调的一点是,人们通常把数据挖掘工具看得过份神秘,认为只要有了一个数据挖掘工具,就能自动挖掘出所需要的信息,这是认识上的一个误区。其实要想真正做好数据挖掘,数据挖掘工具只是其中的一个方面,同时还需要对业务的深入了解和数据分析经验,才能把挖掘出来的知识物化,供决策者参考。另外需要强调的是,任何一种数据挖掘的算法,不管是统计分析方法、神经网络、各种树分析方法,还是遗传算法,没有一种算法是万能的。不同的问题,需要用不同的方法去解决。对于军事方面的数据挖掘来说,也符合以上的规律。

## 参考文献

- [1] 李德毅. 不确定性人工智能. 北京: 电子工业出版社, 2005
- [2] 郑岩峰, 李兴生. 基于数据挖掘的雷达辐射源型号识别. 论证与研究, 2006 年第 2 期, 30-34
- [3] 潘书山, 吴晓云等. 基于粗集理论的武器目标分配. 弹箭与制导学报, 2005, 25 (1) :56-59
- [4] 余舟毅, 陈宗基, 周锐. 基于贝叶斯网络的威胁等级评估算法研究. 系统仿真学报, 2005, 17 (3) :555-558
- [5] A.G.Buchner. Navigation pattern discovery from internet data. In WEBKDD, San Diego, CA, 1999
- [6] W.Lee and S.J.Stolfo. Data mining approaches for intrusion detection. In Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, January 1998

## 作者联系方式

通信地址: 北京市海淀区西三环中路 19 号 35 信箱

邮政编码: 100841

联系电话: 010-66954478 13321175621

# 主动服务和军用分布式数据库应用软件驱动模型研究

李永红 刘东红 罗睿 姜峰

**摘 要:** 本文介绍了主动服务和被动服务的特点,并分析和总结了军用分布式数据库应用软件的主动服务需求,明确了软件驱动模型处于被动服务的现状和根源于数据库管理系统缺乏驱动力的本质,并提出了主动服务模型和建设思路。

**关键词:** 主动服务;数据库;被动服务

## 1 引言

数据和程序的分离是计算机发展中具有里程碑的重大事件,数据库的出现则使得专业数据在方便共享的前提下与应用软件的分离变得更加简单,并且带来了软件的 C/S 结构、三层、多层体系结构等,掀起了数据库应用软件的高潮。

但是,从软件驱动力的角度来仔细分析现有数据库应用程序,可见绝大多数采用的是被动服务模型,在主动性和实时性方面明显落后于主动服务。

## 2 主动服务的基本概念

### 2.1 主动服务

关于主动服务,目前并没有一个准确的、一致的概念。但有三个共同点,第一:主动服务是主动服务观<sup>[1]</sup>的具体实现;第二:从服务的推拉模式来界定主动服务和被动服务,认为“推送”服务是主动服务,而“拉动”服务是被动服务;第三:主动服务是在分布式计算环境下诞生的概念。

本文认为主动服务是要改变传统的“人找数据”为“数据找人”,确定是否主动服务的关键在于源驱动力在分布式计算环境的哪一端,信息交互由谁发起,若由服务器发起,则是主动,否则是被动。从服务效果来看,高质量的主动服务会带来双赢的局面,服务提供者可以进行有效的广告,使用者可以及时掌握最新数据。

### 2.2 主动服务的特点

在“推送”模式应用中,服务器把信息“推

送”给客户器之前,并没有明显的客户请求,“推送”事务由服务器发起。“推送”模式可以让信息主动、快速地寻找用户/客户器,信息的主动性和实时性比较好,应用面广,对用户的技术要求低。但是本文认为也存在如下四个问题。

1) 安全问题。从软件实现角度来看,“推送”模式是一种基于客户/服务器机制,由服务器主动将信息送到客户器的技术,类似于木马的端口反弹技术,给安全带来一定的隐患。

2) 数据风暴问题。当信息提供者将大量信息强制推向用户时,便会将用户淹没于“信息垃圾”中。当然,推送所有的数据不符合应用需求,也不现实。

3) 网络资源浪费问题。推送技术带来新服务模式的同时也引起了网络通信资源的浪费,这是服务器主动发送大量信息或客户代理自动进行信息搜索造成的。

4) 开环问题。“推送服务”通常采用开环方式的通信机制,即信息发送者不关心信息是否已经送达接收者,也无法获得成功发送的标志。所以,难于进行数据反馈和可靠性验证。但是,追求可靠性的系统(例如军事信息系统)通常需要接收方的信息反馈,对信息可靠性进行验证。

### 2.3 被动服务的特点

相对主动服务的是被动服务,被动服务是基于“拉动”模式的。从网络的角度看,拉动服务是基于面向连接的网络协议,提供可靠的数据包传送服务(无错、有序、无丢失),这样虽然简化了信息发布/获取应用程序的设计,针对性强,能满足用户的个性化需求,但本文认为也存在如下六方面不足。

1) 对用户要求较高(例如需用户掌握有关的检索技术)。

2) 及时性差,并不对信息传输的实时性提供保证,因而无法满足某些具有实时要求的应用。例如在进行通告服务时,要求事件的传输具有实时性,需要有支持事件按优先级传输的能力,但“拉动”方式的被动服务无法满足。

3) “拉动”服务要求用户知道所需服务或信息源的准确地址,而在一般情况下,用户是难以知道这些信息的。

4) 在这种被动式的信息服务过程中,用户不得不在网络导航过程中一次次地猜测信息的位置,基本处于无目的状态。这种低效率的信息服务方式无法提供内容及时、质量稳定的服务,很难令用户满意。

5) 查询时间较长。尽管程序员会用尽所有努力(例如优化代码质量,乃至以牺牲代码的模块化程度提供针对特殊需求的特定运行流程等),但是面对的事实仍然是“从大海捞针”,所以,用于获取最新数据或相关信息的数据访问引擎总显得那么不尽人意,迟迟不能返回满意的结果。

6) 查询结果不理想。如果用户不是每次都去修订查询标准,那么按照老的查询标准或许就不能及时获得服务器端的最新数据或相关信息,当然用户也难以知道服务器端是否产生了更有价值的信息,也不知道该怎么修正;即使用户知道该把查询的标准修改成什么,但持续于修改订查询标准,又太麻烦,太浪费时间,特别是战争中的时间。所以花了很大力气,结果却是“在大海里随便捞到的一根难于估量价值的针”。

### 3 军用分布式数据库应用程序的主动服务需求

本文认为军用分布式数据库应用程序的主动服务需求根源于如下五方面需求。

#### 3.1 大众化的需求

作为军事应用系统,战时必然要求能够满足从统帅部到单兵各个层次的信息需求,也即服务要具体到每一单兵,即需要大众化,是一个包含从指挥所的桌面系统到单兵的嵌入式系统得巨型系统。以

COP 为例,嵌入式 COP 中用户的定制需求固然必不可少(例如:拒绝垃圾信息),但 COP 信息定制毕竟太复杂,对用户的水平要求太高(虽然友好的界面是 COP 软件必需的),主动服务具有使用门槛低的特点。所以,“推送”式的主动服务应该是 COP 最主要的服务方式。而且 COP 服务器端拥有丰富的数据资源和优越的计算环境,具备经数据处理产生知识,提供决策支持的能力。若能根据每个用户的需求,向其“推荐”恰当的信息和作战知识,则有助于确保用户的信息优势。

本文也认为,主动服务的思想也是解决目前网格(信息网格作为信息化的基础设施,其发展方向之一就是向用户“推荐”恰当的信息)发展中的瓶颈问题——资源的优化组织和利用的关键技术。

#### 3.2 动态保障的需求

军事信息系统应必须能够适应战场动态变化的需求,这也是所有军事信息系统应该具备的功能。战时必会出现不可预知的状态(美军作战手册里就有明确的一条:“没有任何计划能够在遇到敌人后顺利执行”),需要军用分布式数据库应用程序的客户端和服务端能够自动调整以适应新的战场需求,这就需要双方都具有主动服务的功能。以 COP 可视化为例,当战时出现不可知信源,超越了战场态势可视化的基本类型后,服务器端的 COP 管理员需要即时提供可以让客户理解战场态势的方式,甚至可能是一段 COP 管理员用声音解释不可知信源的录音。所以,必须在 COP 中为用户主动提供战场应急措施。

#### 3.3 实时保障的需求

军事信息系统是指挥自动化系统的重要组成部分,基于时间这一战场最敏感的要害,所以,军事信息系统应是一个实时系统。美军在多次报告里明确强调要加快 COP 的生成速度,满足战场实时性需求,主动服务有较好的实时性。

#### 3.4 自动化的需求

军事信息系统是一个包含多个系统的巨系统,各系统间的消息、数据需要在各节点之间转发。高时效性要求的消息和数据必须自动转发。各系统接收到信息和数据之后能否自动处理或(和)转发,

而减少人工干预是确保时效性的有效方法和手段。这种自动功能的需求就是对主动服务能力的要求。

3.5 保密需求

对于特别重要的信息，例如绝密信息，用户也许根本就不会想到去订购，甚至某些客户端软件的“拉取”功能对于用户来说是保密的，所以就绝对不会去订购，但是，这些信息需要强制广播出去，甚至用户不能拒绝，这时主动服务模型的主动性中自带的广播强制性就特别适用。

4 军用分布式数据库应用软件驱动模型现状

绝大多数大型分布式数据库应用系统的基本模型如图 1 所示。数据库提供者（Data Provider）和数据使用者（Data Provider）之间没有直接联系（即使某些具有实时性要求的系统，也因为实时服

务的不可靠性而未直接在实时信源和应用程序之间建立连接），而是通过数据库进行数据共享。在该模型中，数据库应用软件（Data Consumer）向数据库发送数据请求/指令，数据库解析请求/指令，然后反馈应用软件。

在这个过程中，由于数据库缺乏动力（数据库系统不能触发应用程序 Data Consumer 读取数据，即使 Oracle 提供的服务器端 Java 也需要其他系统来触发）而不能驱动 Data Consumer。所以，当 Data Provider 更新数据库的数据后，除非 Data Provider 通知 Data Consumer，否则 Data Consumer 不知道何时数据库发生了什么变化。为判定数据库是否变化并获得变化后的数据，用户 Data Consumer 不得不采取“连续查询”或者“定时查询”的策略（这也是绝大多数系统的策略）。这样的结果往往是：在有数据到达数据库时用户不能“及时”获得数据；在没有数据到达时因为进行频繁的查询，给数据库服务器带来系统损耗。

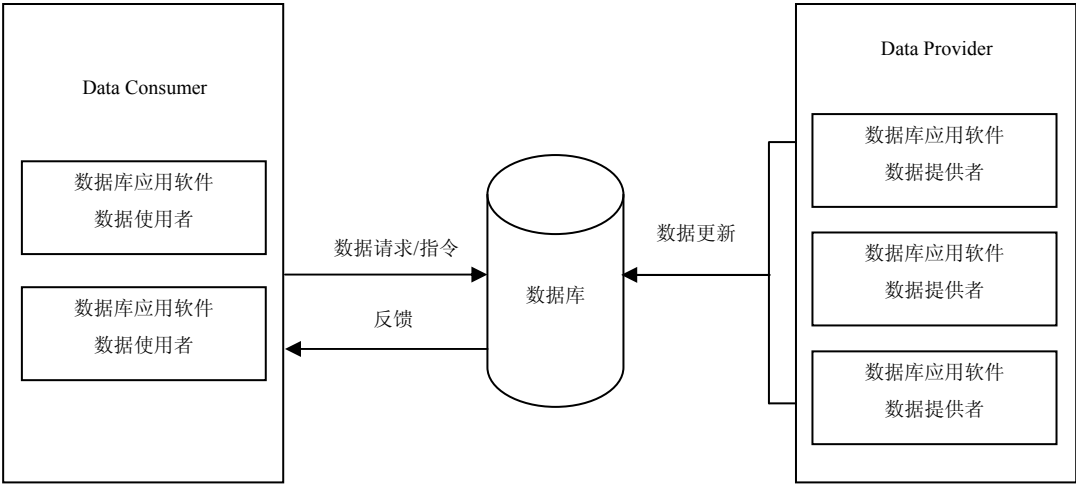


图 1 数据库应用软件的基本驱动模型

用户系统（Data Consumer）是驱动力的来源，数据提供者（Data Provider）提供至数据库的数据，只有等待用户系统来“拉取”，才能够被应用。

5 分布式数据库应用软件的主动服务模式

本文认为，改变数据库被动服务的根本策略应该是：把“连续查询”和“定时查询”变为“及

时”查询，并提出如图 2 所示的改进模型。

在图 2 所示的模型中，Data Provider 对数据库进行数据更新可触发数据库向应用程序发送特定的数据库消息，并且该消息能够被 Data Consumer 接收，Data Consumer 可“及时”对此消息进行处理。

因此，数据库应用程序主动服务模型的关键在于数据库管理系统 DBMS 能否把各种数据库对象（表、视图、存储过程等）的变化转换为可向外部发布的消息并触发应用程序，应用程序要能够捕获

并响应这种变化，以便在数据提供者、数据库、数据使用者之间建立“无延迟”连接。

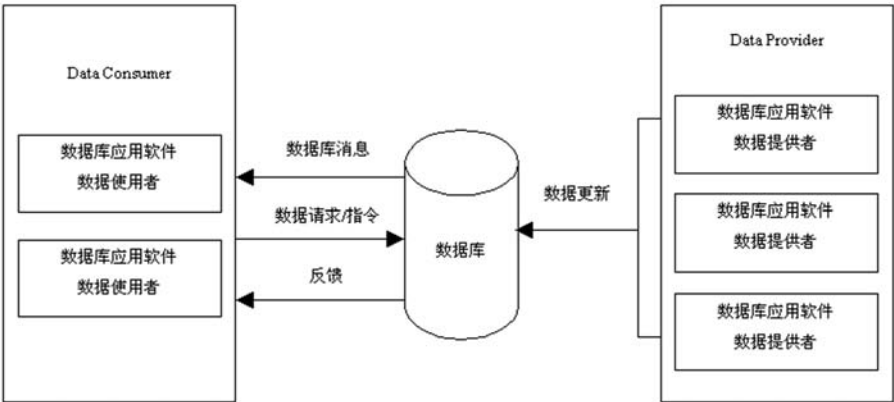


图 2 改进的数据库应用程序的主动服务模型

在当前操作系统、开发语言、集成开发环境、数据库管理系统 DBMS 分别由各公司开发的市场化前提下，为建立能够以主动服务模型运行的数据库应用系统，需要 DBMS 厂商在传统 DBMS 的基础上，建立并完善针对各种数据库对象变化的知识库和事件库，向外部发送能够被应用程序监听并解析的数据库消息。在数据变化驱动应用程序的时候，应用程序仍然可保留系统的部分控制权，软件在开发模式上只需要增加对一个输入信源（数据库消息）的处理即可。

人工智能技术和数据库技术结合的主动数据库技术是目前主动式服务软件的一个热点<sup>[3][4]</sup>，但是也没有从软件驱动力的角度来考虑进行改进，并且研究仍然集中在理论层次，许多概念尚不成熟，技术问题还有待进一步研究解决，还没有成熟的产品。Oracle、Sybase 等数据库厂商虽然接受了主动式服务的思想，但是目前版本（例如 Oracle 10g）的主动性能依然很有限，实现起来很复杂，而且主动功能仅限于数据库内部的主动服务，没有提供向参考文献（略）

作者联系方式

通信地址：北京市丰台区大成路 13 号 R02  
邮政编码：100039  
联系电话：010-66820295-825 13520219161

外部发送数据库消息的能力，不能够驱动应用程序，不支持主动服务模型。

6 结束语

本文仅从软件驱动模型进行了分析，得出了大型分布式数据库应用软件以主动服务模型运行的必要性，提出了简单的运行模型和建设以主动服务模型运行的军事信息系统的简单建议，所作的技术试验很有限，对主动服务的认识还不够深刻。但是，在软件人员不得不承认软件工程迄今没有建立起公理化系统，尚不能给人以类似物理、化学等具有严密数学基础的科学的信赖感之前，在软件工程还处在一个正在生产可能存在很多不确定性的未经充分验证乃至实战检验的软件阶段，军事信息系统的用户使用需求应该得到足够的重视，因为用户至上思想是主动服务的精髓。

# 基于IRP的军队信息资源开发利用

梁春雨 李振富 李东 吴垚

**摘 要:** 本文介绍了军队信息资源开发利用的相关概念,指出它在军队信息化中的核心地位和主要任务。通过分析其发展现状和存在问题,倡导运用现代信息工程理论和 IRP 技术来解决军队数据管理危机中的“信息孤岛”问题,最后给出了军队信息资源规划的工程方案和基本框架,其成果概括为:“建立两种系统模型和一套数据基础标准”。

**关键词:** 军队信息化;信息资源开发利用;IRP;信息资源规划

军队信息资源是打赢信息化战争和建设信息化军队不可或缺的军事战略资源。全军信息化工作会议中已经明确提出:“军队信息化工作的核心是信息资源开发利用”。信息资源是发挥高技术武器装备性能的“粘合剂”,是战斗力生成的“催化剂”,没有军队信息资源的开发利用,搞军队信息化建设就等于无源之水、无本之木。

## 1 军队信息资源开发利用的重要地位和主要任务

### 1.1 军队信息资源开发利用的基本概念

军队信息资源开发利用是指在军队各项工作领域中运用现代信息技术采集、处理、传递和高效利用各种信息资源,来提升部队作战效能的过程。开发是基础,利用是目的;军队信息化围绕信息展开,通过开发利用信息资源来整合作战体系,来提升作战能力,来提高管理水平;军队信息资源是在各项军事活动中产生积累的、经过加工处理的、有序化的、有用信息的集合。具有海量、涉密、对抗、无序、易毁等特点,按内容划分,有作战指挥信息、训练教育信息、政工管理信息、后勤装备信息等;军队信息资源规划是指对各项军事实践活动中产生和需要的信息,从采集、处理、传输和使用的全面规划。其主体是总体数据规划<sup>[1]</sup>。

### 1.2 军队信息资源开发利用是军队信息化的核心任务

(1) 是军队信息化的本质要求

军队信息化必然要求对信息资源的深度开发和高效利用,发挥信息主导作用,实现信息资源对其他资源的节约、整合、增值、创新功能。从而提高军队工作效率、建设效益和作战效能,最大限度地谋取信息优势、决策优势和行动优势,最终增强信息化条件下的作战能力。

(2) 是提升联合作战能力的迫切需要

由于我军信息资源开发不足、采集重复、维护更新滞后、信息共享困难、利用水平低,已经成为制约联合作战部队武器平台之间实现互通、互联、互操作的“瓶颈”。信息资源是战斗力的重要构成要素,离开了信息资源的有效开发利用,无论硬件、软件建设多么先进,都不可能进入实用、发挥效益。

(3) 是当前军队信息化的工作重心

重点解决信息资源开发利用滞后于信息基础设施发展的问题,信息应用系统建设要围绕其开展,系统综合集成要以数据集成为重点,所以它是检查衡量信息化工作成效的重要指标。

### 1.3 军队信息资源开发利用的主要工作任务

目标就是通过统一标准规范、构建共享环境、丰富信息内容、完善运行机制,实现军队信息资源的优化配置与高效安全利用。军队信息资源开发利用的主要任务有五项<sup>[3]</sup>。

(1) 开展作战需求牵引和信息资源规划的顶层设计

以军队建设和作战需求为牵引,发挥部队的主导作用,以应用促进开发,以开发带动应用,使信息资源的内容、格式、存储方式、传输流程都要符合作战要求。各总部、军区、军兵种在全军总体设



计下进行信息资源规划,以信息工程理论为指导,构建总体规划框架,开展专项数据工程建设。

(2) 加强军队信息资源开发利用的标准化工作  
统一制定信息资源分类与编码标准、国防数据词典系统、通用数据模型和信息资源目录体系,强化标准化工作的集中管理和监督检查,逐步建立全军统一协调的信息资源标准化体系及动态数据管理机制。

(3) 加快军队信息资源内容建设

依据总体规划和急用先建,重点建设人员、地理空间等基础数据库,集中抓好联合共享数据库建设,完善业务部门专业数据库。按照“一数一源”原则,保障信息内容的可靠性和质量,不断充实完善军队信息资源内容。

(4) 积极推动军队信息资源共享

建设全军信息资源交换体系,实行授权性分等级的安全共享机制,科学确定各级、各部门信息共享的内容、范围、等级和共享方式、共享责任。打破信息“壁垒”,积极推广网上推演、网上训练、网上办公。

(5) 落实军队信息资源安全保密工作

统筹规划和同步实施安全保密建设,技术防护与安全管理并重,容灾备份与应急机制相结合,专业队伍重点防护与全员全程防护并举,构建完善的信息资源安全防护和保密体系。

## 2 军队信息资源开发利用现状及问题分析

### 2.1 我军信息资源开发利用的基本现状

(略)

### 2.2 部队信息资源开发利用的突出问题

(1) 军队信息资源的数据源质量较差

各部门分头建设的小型数据库比较多。由于数据维护滞后和更新不及时,信息查询功能弱,无法实现分级访问控制,数据“保鲜”程度低,“死库”或“半死库”比较多。

(2) 军队信息资源重复采集问题普遍突出

信息资源开发利用长期以来处于“自采自用”的低层次状态,缺乏横向协调、互补和支援。如:全军人员实力统计,军务、组织、干部、战勤、财

务等部门均按照各自的需求分头采集上报,造成重复劳动和统计结果的不一致。

(3) 部队大量配发的办公应用系统功能单一

部队在用的应用系统多数集成化程度不高,面向部队、功能集成的应用软件很少。由于一个系统只能处理一项业务工作,大量配发的互不兼容业务系统严重影响部队的工作效率。

(4) 信息资源开发利用标准体系尚未全面建立直接制约了信息资源的交换与共享

由于缺乏跨领域、跨部门的统一技术体制和信息编码标准,加上各部门开发时各自为政,没有依据标准进行数据源建设,导致信息资源在互联、互通、互操作方面存在的问题非常突出,导致目前各级部队形成了无数的信息“孤岛”。

(5) 军队信息资源安全防护漏洞大带来较大隐患

特别是信息安全核心技术受制于人,限制了网络信息资源的开发利用。军队信息资源具有很强的保密性,其共享和使用必须在安全保密的前提下进行,否则就会适得其反。

## 3 基于IRP的军队信息资源规划的工程方案

军队信息资源规划是基于信息工程方法论进行的全军信息资源规划,即按照工程化步骤和相应标准规范,利用有效的工具技术进行各职能域的信息需求和数据流分析,制定军队数据管理基础标准,建立系统的信息系统框架——功能模型,数据模型和系统体系结构模型。

军队信息资源规划的工程方案由理论方法、标准规范和软件工具构成,主要成果可以概括为:“建立两种模型和一套标准”。“两种模型”是指系统的数据模型和功能模型,“一套标准”是指信息资源规划的基础标准。

### 3.1 军队数据管理的危机和转机--信息工程方法和IRP工具

由于军队信息化发展的阶段性,普遍存在着重硬轻软、重网络轻数据;加上部队追求“实用快上”的分散开发、孤立设计、数据自采自用;系统间的接口数目随着新的应用项目的增加而按几何级

数增加，仅靠增加接口数目的方法实现系统集成是不可能的。最终全军形成无数互不兼容的应用系统、指挥平台、“信息孤岛”丛生，使军队信息化建设陷入了“数据处理危机”。为此必须采取冲出孤岛的“治本之策”——进行“军队信息资源规划”。

信息工程方法论（简称 IEM）。由詹姆斯·马丁（James Martin）提出的一整套信息化理论与方

法<sup>[4]</sup>。基本原理有三条：数据位于现代数据处理系统的中心；数据结构是稳定的，处理是多变的；最终用户必须真正参加开发工作。他还提出四类“数据环境”：数据文件、应用数据库、主题数据库和信息检索系统。主题数据库都由基本表构成，基本表具有原子性、演绎性和规范性。集成化的军队信息系统要建立在高档次的数据环境之上就必须进行信息资源规划。它的体系结构图如图 1 所示。

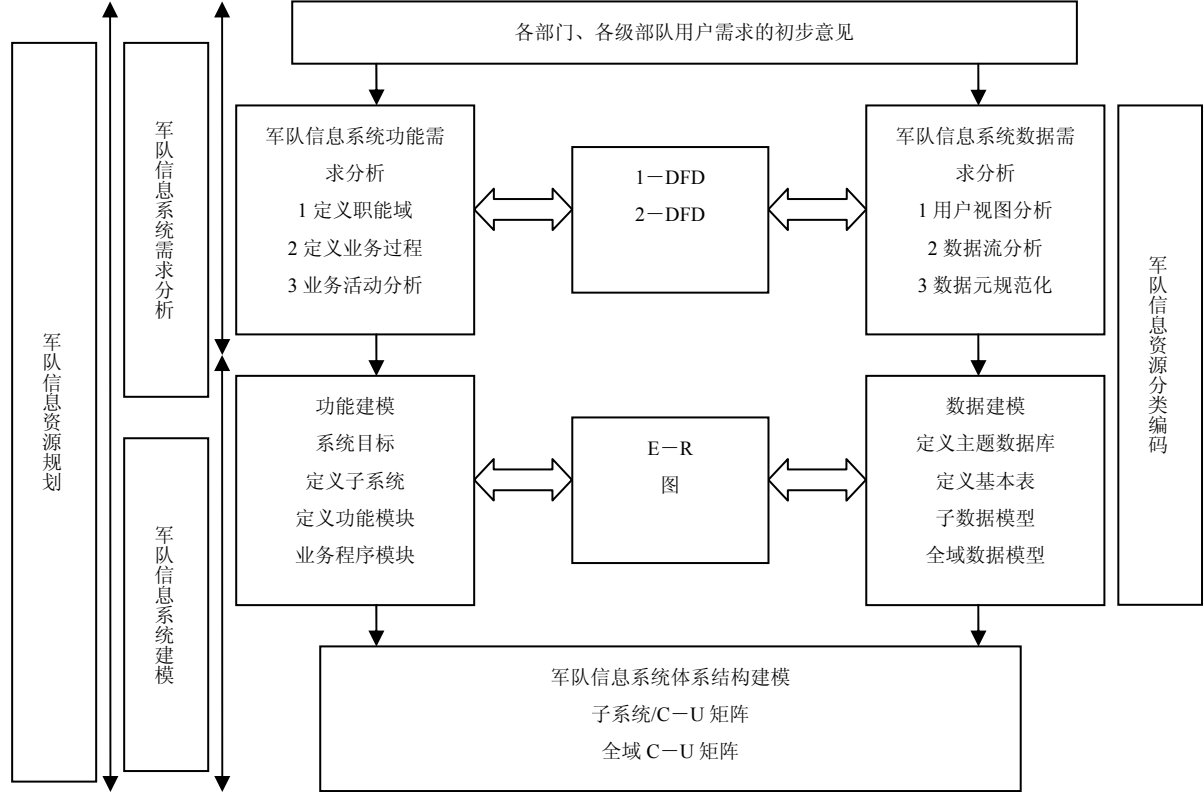


图 1 信息资源规划总体结构图

信息资源规划软件工具 IRP2000 主要用于支持企业信息资源规划的需求分析、系统建模和信息资源管理基础标准的建立。共包含七大功能模块：① 企业规划模块；② 业务功能分析模块；③ 业务数据分析模块；④ 系统功能建模模块；⑤ 系统数据建模模块；⑥ 系统体系结构建模模块；⑦ 系统元库管理模块。

3.2 军队信息资源规划的需求分析和系统建模技术

(1) 需求分析技术

需求分析是信息资源规划的第一阶段，包括对业务的需求分析和对数据的需求分析。业务的需求分析的技术方法是通过业务过程矩阵，关键因素分

析（CSF）方法利用“职能域—业务过程—业务活动”的层次结构得到业务模型。即首先确定职能域模型，然后识别定义每个职能域的业务过程，最后列出每个业务过程的各项业务活动。数据的需求分析也叫用户视图分析。用户视图是一些数据的集合，它反映了最终用户对数据实体的看法，主要使用编码技术和范式理论。可分为两步进行：用户视图分类和登记以及用户组成分析。最后结合一二级职能域数据流图，进行各种数据流的量化分析。通过频度分析提取出共享度高的数据元，它是最小的不可再分的信息单位，这些元素的标准化尤为重要。

(2) 系统建模技术

系统建模是需求分析的继续和“定型”，是信息资源的总体的概括和描述，包括功能建模，数据

建模和系统体系结构建模。功能建模是对系统功能的概括性表示,一般采用“子系统—功能模块—程序模块”的层次结构来描述;数据建模是建立信息组织的框架和进行信息的组织。一般是通过 E-R 图和数据库范式理论建立全域数据模型和子系统数据模型。数据模型的基本模块是“基本表”,是由数据元素构成的达到三范式的数据结构,是系统集成和信息共享的基础。最后系统体系结构建模就是建立系统数据模型和功能模型的关联结构,它决定着共享数据库的创建与使用,也是进行数据分布分析和制定系统开发计划的依据,这种关联结构通常采用 C-U 矩阵来表示。信息资源规划的各组成部分,过程及主要技术见文献[2]。

### 3.3 军队信息资源规划的基础标准规范

#### (1) 数据元素标准

数据元素是最小的不可再分的信息单位。数据元素的定义用来描述其意义和用途,结构为“修饰词—基本词—类别词”。而名称是指它的代码,是计算机和人共同使用的标识。数据元素的名称和定义在全系统中要保持一致,要控制同名异义和同义异名的数据元素使用。

#### (2) 信息分类编码标准

它的对象是一些最重要的数据元素,它们决定着信息的质量和效率。应参照国家有关标准(GB7026—86)结合部队实际,尽快建立健全全军通用的信息分类编码标准。它的对象大体分为三种: A 类编码对象:代码表寓于基本表的编码对

象; B 类编码对象:在应用系统中不单独设立代码表的较大编码对象; C:在应用系统中使用频度很高的短小的编码对象。

#### (3) 用户视图标准

它是一组数据元素的抽象,反映了最终用户的信息需求和对数据实体的看法。主要包括单证,报表和屏幕格式等。规范简化有用的用户视图命名,分类编码和组成结构,是信息系统进行内外信息交换所必需的过程,也是导出主题数据库的基础。

#### (4) 概念数据库标准

概念数据库是最终用户对信息系统中存储数据集合的看法,反映了用户的综合性信息需求,一般用数据库名称及其内容描述或数据项列表的方式来表达。建立规范化的概念数据模型,需要广泛深入的分析,识别,定义出各个数据库的名称和信息内容。

#### (5) 逻辑数据库标准

逻辑数据库是系统分析设计人员的观点,是对概念数据库的进一步分解和细化,它是由一组规范化的基本表组成的。采用简化的结构化 E-R 图来表达,包括各基本表的标识,名称,主码和属性列表,以及基本表之间的关系。上述五项标准构成了数据管理的标准化体系。

目前部队信息化建设提出了实现系统集成的要求,正好是信息资源规划的最佳时期。我们必须抓住这一时机,搞好军队信息资源开发利用,解决分散信息系统集成化问题,为使军队信息化走出徘徊不前的局面奠定坚实的基础。

#### 参考文献(略)

#### 作者联系方式

通信地址:西安市王曲镇西安通信学院

邮政编码:710106

联系电话:029-84706828 13572554163

# 一种基于小波变换的认知无线电频谱感知方法

林生森 吴启晖 盛雁鸣

**摘 要：**在认知无线电系统中，认知无线电设备需要不断的对频谱进行感知。频谱感知技术是认知无线电系统的关键技术，文章研究了基于小波变换的频谱感知方法，该方法通过小波变换实现初步的频谱感知。文章在该方法的基础上进行了改进，利用不同尺度下信号小波变换的相关性，进一步抑制噪声。仿真表明，改进方法增强了频谱感知的抗噪声性能。

**关键词：**认知无线电；频谱感知；小波变换

## 1 引言

随着通信的发展，频谱资源越来越紧缺。研究表明，许多已分配的频谱并没有被充分利用<sup>[1]</sup>。若能对这些“未充分利用”频谱进行再利用，可以在很大程度上提高频谱的可用容量。近年来出现的认知无线电技术是一种能够感知周围无线环境的新颖智能无线通信技术，能避开正在使用的频道，动态地分配频率<sup>[2]</sup>，能够有效地解决频谱接入问题。认知无线电在军事上也会有极其广泛的应用。军事通信也面临巨大的频率分配问题。有了认知无线电，军事通信也将不再局限于一个静态的频率规划，可以从根本上适应需求的变化。

频谱感知技术是认知无线电的关键技术，频谱感知的目的就是快速检测出未被授权用户占用的频段。已有许多文献研究了频谱感知方法，比如匹配滤波检测<sup>[3][4]</sup>，能量检测<sup>[3][4]</sup>，特征检测<sup>[3][5][6]</sup>等。匹配滤波是一种最优的检测方法，但它的缺点是必须具备被检测信号的先验知识。能量检测法是一种简单的信号检测方法，不需要任何先验知识，但易受噪声的影响。循环平稳特征检测是考察信号的循

环谱来检测信号，它的检测精度高，但其计算相对复杂。实际中更倾向于综合使用上述方法。如文献[7]中，提出了一种两步模式的频谱感知结构。该结构首先通过能量检测对宽带频谱进行快速的初步感知，剔除高能量频段，得到较低能量的待选频段集，对待选频段集再进行更为精确的检测例如循环特征检测。

文献[8]也提出了初步感知和精确感知相结合的结构，提出利用模拟域的小波变换进行初步感知。模拟域小波变换的优点在于速度快，只需要低速的模数转换器。本文致力于研究初步感知，针对文献[8]中的小波变换感知方法进行了改进，提高了其抗噪声性能。

## 2 小波变换频谱感知方法

小波变换系数表示了信号与某一特定小波的相关程度。文献[9]指出，通过调整小波窗口大小和载频，可以得到不同尺度下小波变换系数，小波变换系数可以表示信号谱分量。文献[8]给出了基于小波变换的频谱感知接收结构，如图1所示。

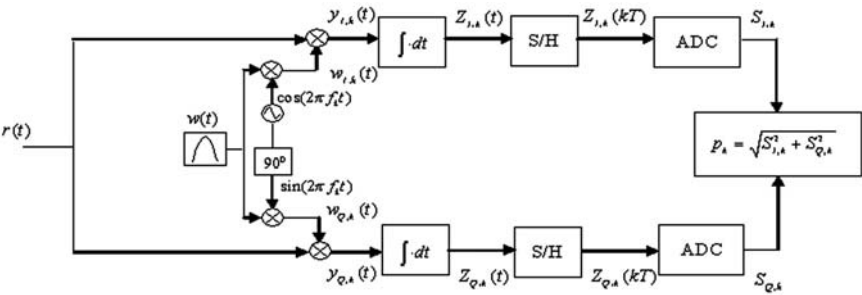


图1 小波变换频谱感知接收结构图（摘自文献[8]）

该结构包括小波信号产生器、乘法器、积分器以及低速的模数转换器。因为整个感知过程大多在模拟域完成, 所以其感知速度非常快, 可以实现频谱的实时感知。接收信号与小波信号相乘, 相当于对接收信号进行了带通滤波, 一定程度上抑制了部分噪声。

文献[8]的感知原理过程如下所述。

小波信号产生器产生小波信号  $w(t)$ , 由  $w(t)$  生成正交两条支路信号  $w_{I,k}(t)$ 、 $w_{Q,k}(t)$ ,

$$w_{I,k}(t) = w(t) \cdot \cos(2\pi f_k t) \quad k=0, \dots, N \quad (1)$$

$$w_{Q,k}(t) = w(t) \cdot \sin(2\pi f_k t) \quad k=0, \dots, N \quad (2)$$

其中  $N = \text{Round}[(f_{\text{stop}} - f_{\text{start}}) / f_{\text{sweep}}]$ ,  $f_k = f_{\text{start}} + k f_{\text{sweep}}$ 。

$f_{\text{start}}$ 、 $f_{\text{stop}}$  分别为待感知频段的起始和结束频率。 $f_{\text{sweep}}$  为感知步长。 $B_w$  表示小波的带宽, 小波带宽的大小影响感知的分辨率。整个频段的感知时间与小波带宽以及感知步长的关系如 (3) 式, 其中  $T_w$  为小波时域窗长。

$$T_{\text{total}} = T_w \cdot N \propto \frac{1}{B_w} \cdot \frac{1}{f_{\text{sweep}}} \quad (3)$$

接收信号与两支路小波信号的相关分量为

$$Z_{I,k}(t) = \frac{1}{T_w} \cdot \left\{ \int_{kT_w}^{(k+1)T_w} [r(t) \cdot w_{I,k}(t)] \cdot dt \right\} \quad (4)$$

$$Z_{Q,k}(t) = \frac{1}{T_w} \cdot \left\{ \int_{kT_w}^{(k+1)T_w} [r(t) \cdot w_{Q,k}(t)] \cdot dt \right\} \quad (5)$$

这两个相关分量表示了接收信号在频率  $f_k$  上的谱分量。通过低速模数转换, 得到离散化的相关分量值  $S_{I,k}$  和  $S_{Q,k}$ , 最后以幅值  $p_k$  表示信号频率  $f_k$  的谱密度

$$p_k = \sqrt{S_{I,k}^2 + S_{Q,k}^2} \quad (6)$$

### 3 改进的小波变换感知方法

上述频谱感知结构实际是将接收信号在小波信号上进行投影, 但上述结构中小波信号带宽  $B_w$  是固定的, 即在接收信号的各个频段上进行相同尺度的小波变换, 这样就难以体现小波多尺度变换的特点。另外实际中如果没有信号的先验知识难以调整最佳的小波窗口长度适应信号来控制感知时间。

在图像处理等领域经常采用基于小波变换尺度

间相关性的去噪方法。信号的小波变换在各尺度间具有较强的相关性, 而噪声在各尺度间没有明显的相关性。基于小波变换尺度间相关性的去噪正是利用这种相关性滤除噪声的小波系数, 达到去噪的目的。

因此可以考虑利用信号小波变换尺度间的相关性对文献[8]的感知方法进行改进, 进一步增加其抗噪声性能。文献[10]指出, 基于小波变换尺度间相关性的去噪方法计算量较大。针对频谱感知的应用背景, 只计算两个不同尺度间的小波变换的相关分量。两个不同尺度分别记为  $a$ 、 $b$ , 小波带宽分别为  $B_{wa}$ 、 $B_{wb}$ 。根据图 1 的频谱感知结构分别在尺度  $a$ 、 $b$  上以相同的步长进行频谱感知, 再将两个尺度下感知的谱密度函数进行相关运算, 算法具体过程如下。

1) 尺度  $a$  下接收信号在  $I, Q$  两支路小波信号上的投影分量,

$$Z_{a,I,k}(t) = \frac{1}{T_{a,w}} \cdot \left\{ \int_{kT_{a,w}}^{(k+1)T_{a,w}} [r(t) \cdot w_{a,I,k}(t)] \cdot dt \right\} \quad (7)$$

$$Z_{a,Q,k}(t) = \frac{1}{T_{a,w}} \cdot \left\{ \int_{kT_{a,w}}^{(k+1)T_{a,w}} [r(t) \cdot w_{a,Q,k}(t)] \cdot dt \right\} \quad (8)$$

2) 离散化得到离散化分量

$$S_{a,I,k} = Z_{a,I,k}(kT_{a,w}) \quad (9)$$

$$S_{a,Q,k} = Z_{a,Q,k}(kT_{a,w}) \quad (10)$$

3) 则尺度  $a$  下的谱密度函数为

$$p_{a,k} = \sqrt{S_{a,I,k}^2 + S_{a,Q,k}^2} \quad (11)$$

同样可以得到尺度  $b$  下的谱密度函数

$$p_{b,k} = \sqrt{S_{b,I,k}^2 + S_{b,Q,k}^2} \quad (12)$$

4) 将两个尺度下的小波变换进行相关运算, 得到新的谱密度函数

$$p_{\text{corlate},k} = p_{a,k} \cdot p_{b,k} \quad (13)$$

对于接收信号, 用户信号频段内的小波变换系数相对较大, 噪声的小波变换系数趋于白化。在不同的小波尺度下, 信号频段内的小波变换系数相关性强, 噪声的小波变换系数几乎不相关。通过两个尺度的相关运算, 增加了信号的小波系数, 抑制了噪声。改进方法不需要改变文献[8]的频谱感知结构, 只是增加了两个尺度的相关运算, 几乎不增加硬件系统的复杂度。实际中为增加感知的稳定性, 可以进行多次平均, 得到的谱密度函数为

$$P_{\text{corlate},k} = \left( \frac{1}{N_{\text{Avg}}} \right) \cdot \sum_{n=1}^{N_{\text{Avg}}} p_{\text{corlate},n} \quad (14)$$

## 4 仿真分析

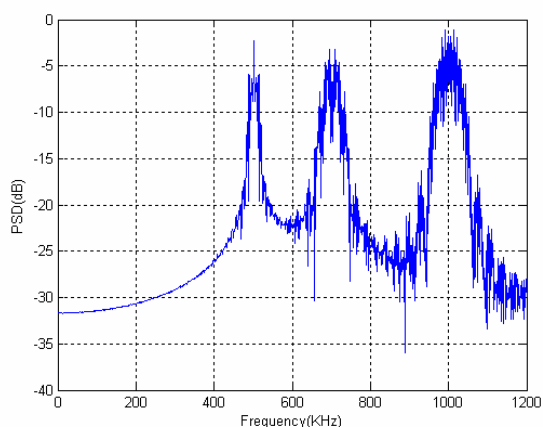
假设认知设备待感知频段为 0-1.2MHz，在该频段存在三个用户信号，用户 1 信号  $s_1(t)$ ，用户 2 信号  $s_2(t)$ ，用户 3 信号  $s_3(t)$ 。认知设备的接收信号为

$$f(t) = s_1(t) + s_2(t) + s_3(t) + n(t) \quad (15)$$

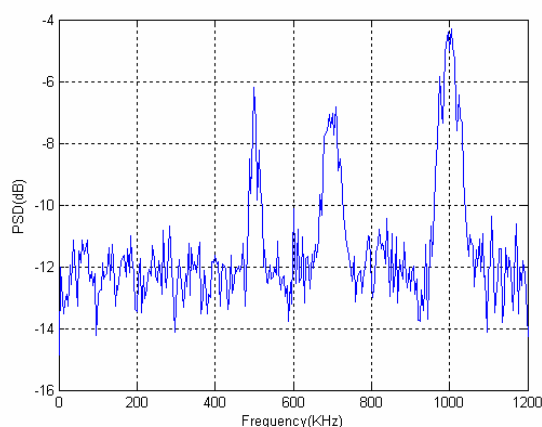
其中  $n(t)$  为零均值高斯白噪声。

用户信号中心频率分别为 500KHz、700KHz、

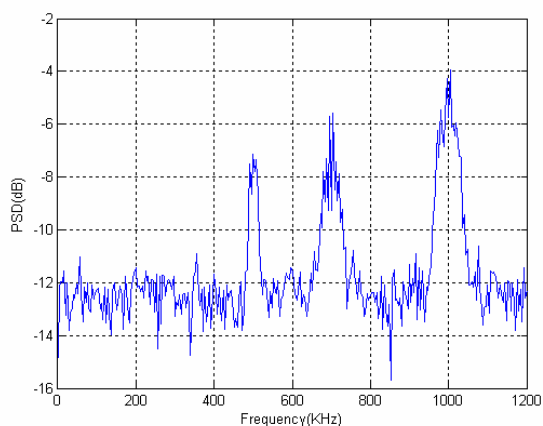
1MHz，调制方式为 BPSK，所占带宽分别为 50KHz、100KHz、120KHz。接收端对于各用户信号的接收信噪比分别为 -8dB、-5dB、0dB。尺度 1 的小波带宽  $B_{wa}$  为 9KHz，尺度 2 的小波带宽  $B_{wb}$  为 6KHz，感知步长  $f_{sweep}$  为 4KHz。图 2 (a) 为无噪声污染情况下的有限时间接收信号谱密度函数，只采用尺度 1 的谱密度图如图 2 (b) 所示，图 2 (c) 为尺度 2 下的谱密度图，采用改进方法的谱密度图如图 2 (d) 所示。



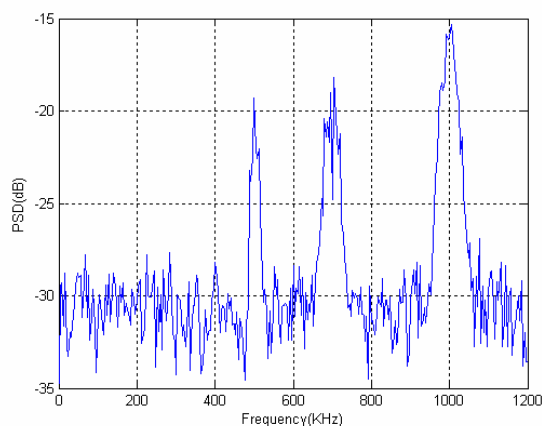
(a) 无噪声下谱密度图



(b) 尺度 1 下谱密度图



(c) 尺度 2 下谱密度图



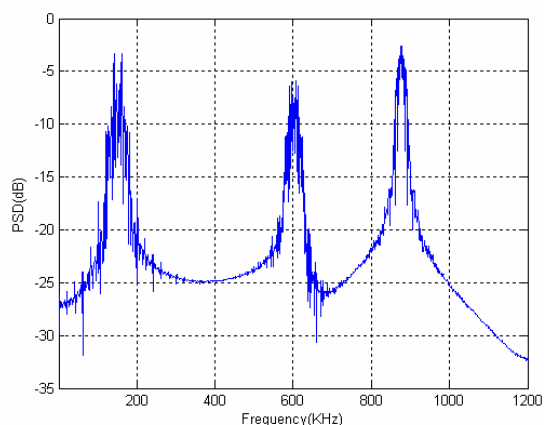
(d) 改进方法下的谱密度图

图 2 仿真分析 1

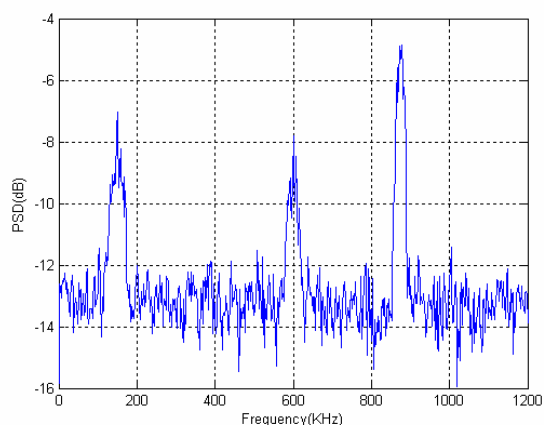
尺度 1 和尺度 2 分别进行了 10 次感知，然后进行平均。改进方法分别进行了 5 次尺度 1 感知和 5 次尺度 2 感知。由 (3) 式可知改进方法的感知时间介于尺度 1 和尺度 2 之间。可以看到，改进方法使噪声电平大约降低了 5dB。用户信号所占带宽部分变得更加明显。改进算法增强了抗噪声性能。

用户信号中心频率分别为 150KHz、600KHz、875KHz，调制方式为 BPSK，所占带宽分别为

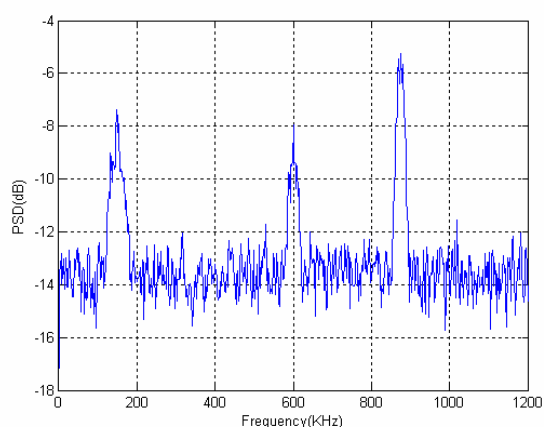
80KHz、64KHz、50KHz。接收信噪比分别为 -6dB、-9dB、-2dB。尺度 1 的小波带宽  $B_{wa}$  为 6KHz，尺度 2 的小波带宽  $B_{wb}$  为 2KHz，步长  $f_{sweep}$  为 2KHz。同样各尺度进行 10 次感知，改进方法两尺度各进行 5 次，得到的各谱密度函数如图 3 所示。



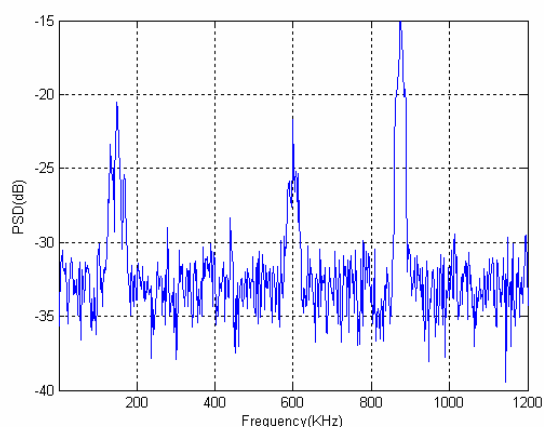
(a) 无噪声下谱密度图



(b) 尺度1下谱密度图



(c) 尺度2下谱密度图



(d) 改进方法下的谱密度图

图3 仿真分析2

## 5 结束语

频谱感知对于实现认知无线电至关重要, 如何高效的进行感知一直是研究的热点。本文研究了基于模拟域小波变换的感知方法, 在其基础上提出了两尺度相关的改进算法。改进算法利用不同尺度下信号小波变换的相关性增强了抗噪声性能。仿真表明, 改进算法性能有较大提升。

参考文献 (略)

作者联系方式

通信地址: 江苏省南京市御道街标营2号移动通信教研室

邮政编码: 210007

联系电话: 025-80828495

# 创新的网络体系结构--4D模型

刘伟 杨林 戴浩

**摘 要:** 本文介绍了目前针对网络体系结构研究的现状, 重点对革命式发展路线中的 4D 模型进行了介绍。分析了现有的网络控制功能平面的划分与不足, 4D 模型依据三个设计原则, 将现有的三个网络控制功能平面进行整合, 重新划分为四个功能平面, 本文对此进行了详细的介绍, 最后说明了 4D 模型的优点。

**关键词:** 网络体系结构; 4D 模型; 网络控制功能

## 1 引言

30 多年来, 互联网有了巨大的发展, 从 1969 年只有 4 台计算机互连的 ARPANET 网络, 逐渐演变为现有的超过 2 亿台主机的大规模复杂信息系统, 并且还在以超摩尔定律的速度继续发展。网络规模不断膨胀, 网络结构日益复杂, 网络应用层出不穷, 网络安全问题日益突出, 管控网络的能力越来越弱, 而很多安全隐患正是源于对网络可控可管性的近乎丧失。

IP 网在设计之初, 所面临的主要需求是互连互通, 因此, 采用了端到端无连接的分组交换以及尽力而为转发的原则。然而新的应用对网络体系结构提出了许多新的需求, 使得传统的互联网网络体系难以适应网络的发展。尽力而为的原则不能保证服务质量, 特别是流媒体所要求服务质量; “边缘论”和无连接的体系结构导致网络控制手段薄弱, 无法有效地为用户提供满意的安全保障; 复杂异构的多网互连, 庞杂的协议体系和海量通讯信息所带来的交互复杂性, 使得网络维护复杂, 管理成本高, 可扩展性差, 这些都迫使我们不得不重新审视互联网的体系结构, 甚至是考虑进行革命性的变革。

## 2 两种发展路线

目前, 对互联网体系结构的研究主要有两种发展路线: 一种是修补式的渐进路线, 通过不断增加新的协议来应对新应用; 而另一种是革命式的路线, 依据未来的网络需求和当前网络的弊端, 重新

设计互联网的体系结构。从零开始的革命路线是非常必要的, 因为仅在现有的网络体系结构上进行修补, 而不改变体系结构中阻碍互联网发展的设计原则, 是无法从根本上解决问题的, 只能处于不断地出现问题, 不断地解决问题, 又不断地出现亟待解决的新问题这样一个周而复始的局面; 并且, 修补改造后的体系结构变得复杂而脆弱, 难以理解和把握, 有失控或者崩溃的危险, 甚至很有可能出现一些无法用补丁解决的问题。

探寻新的网络体系结构, 研究下一代网络逐步成为了国内外关注的焦点, 并且将是各国网络发展的趋势。我国在《国民经济和社会发展规划纲要》中提出要构建下一代互联网, 健全信息安全保障体系。《国家中长期科学和技术发展规划纲要(2006-2020 年)》的优先主题中, 也指出要研究下一代网络关键技术与服务。学术界方面, 2002 年的 973 项目中, 就包括了“新一代互联网体系结构理论研究”这一课题, 已研究并提出了新一代互联网体系结构必须包含的五个基本要素和构建“基于 IPv6 真实地址的可信任新一代互联网”的重大创新。

美国国家科学基金会启动了一个名为“全球网络环境创新”(GENI)的项目, 它不再是渐进式地改进当前的互联网, 而是要重新设计互联网, 打造一个更适合未来计算环境的下一代互联网。贝尔实验室的 SoftRouter 项目, 其目标是设计新的体系结构将路由器中软件实现的控制逻辑与硬件实现的转发逻辑分离。欧洲的 Ambient 项目旨在提出一种新的网络控制体系结构, 尤其适用于具有大量特殊要求的移动互联网络。

“网络控制与管理的全新 4D 模型”是卡内



基·梅隆大学牵头提出的研究项目，其主要思想是对现有网络的体系进行改进设计，从而提高网络的可控性。其研究表明，目前网络的脆弱性和难以管理问题的根本原因在于控制和管理层面的复杂性，即协调各种网络元素的软件和协议十分复杂，特别是决策逻辑和分布式系统纠缠在一起。下面重点介绍 4D 模型。

### 3 4D模型简介

#### 3.1 传统网络功能平面的划分

根据网络担负的功能，传统的通信网络和互联网可被分为三个平面，如图 1 所示：

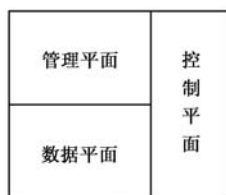


图 1 传统网络功能平面的划分

1) 数据平面：数据平面负责数据包转发，路由器根据最长地址前缀匹配原则确定每个数据包的出链路，并依据访问控制列表对数据包进行过滤。另外，数据平面还实现队列管理以及地址转换等功能。

2) 控制平面：控制平面由确定数据平面状态的分布式算法组成。例如，控制平面包括 BGP 更新消息以及 BGP 决策过程，还包括 IGP（例如 OSPF）使用的 Dijkstra 最短路径算法。控制平面的一个最主要的工作就是计算 IP 子网间的路由，通过综合每个路由协议的路由信息库（RIB）构造出转发信息库（FIB），以做出数据包转发决策。在互联网中，控制平面和数据平面是交织在一起的。

3) 管理平面：管理平面监视网络，配置数据平面及控制协议。管理平面存储和分析网络的度量数据，例如收集和综合 SNMP 统计表，流量记录，OSPF LSA，BGP 更新流等。管理平面还为满足流量工程的目标配置 OSPF 链路权重和 BGP 策略。同样，通过分析流量来检测拒绝服务攻击和配置 ACL 来阻止恶意访问也是管理平面的工作。

传统网络功能平面划分的不足在于：①路由器中控制决策和数据转发捆绑，负担沉重。研究显示为了保障网络的互连互通，需要在网络中的所有路

由器配置几十万行的命令，导致的结果必然是一个复杂的、容易出现故障的网络。②协议设计严格分层，决策控制逻辑冗余。分层的设计方法在有线固定通信网络协议设计中效果很好，但并不适合于无线网络。并且由于每个路由器和交换机都隐含地嵌入了一些决策逻辑，使得多实体参与的分布式决策算法的实现与消息传递的分布式系统问题交织在一起。③网络状态信息分散，网络连接状态不一致。多种协议共存于同一个交换机/路由器，共同影响最终的控制信息，造成不同交换机/路由器的控制信息不同步或不一致，并且与全网决策的目标是对立的。

#### 3.2 4D的三个设计原则

过去几年，进行网络研究的学者达成了一个共识，即：IP 网络的控制和管理必须依据全网的策略信息来驱动。但是控制和管理平面的功能划分方法对网络管理并没有任何显著的推进作用，网络管理员还是必须在每个路由器上具体地配置参数，键入命令，间接地响应全网的抽象策略并对操作行为进行限制。因此，必须将每个路由器中的这一部分功能改变为直接支持全网级的抽象，实现全网的自动管理，即对网络操作行为的限制必须能直接地表达出来，然后自动地（通过协议）转化为对每个路由器具体规划。因此，必须进行功能的重整，并提出了三个关键原则，即网络目标、全网视图以及直接控制。

1) 网络目标：必须根据各网的特殊性能需求及目标制定全网一致的策略或目标。例如：一个可达性策略的目标可以表示为：“不允许子网 B 内的主机访问子网 A 中的日志服务器”。但是，现有的网络需要将这个目标转换为各个路由器的配置命令，实现从网络目标到低层实现机制的转换，其间难免会出现语义转换的失误，在最终实现时就有可能违背原定的目标。

2) 全网视图：全网视图的概念是借鉴于数据库通信，意为能够全面了解网络中每个元素的状态。掌握及时、准确、全网视角的拓扑结构、流量以及事件对于维护和管理一个鲁棒网络是至关重要的。全网的视图必须准确地反映数据平面当前的状态，包括每个设备的信息，包括它的名字，资源限制以及物理属性等。但是，现在的控制层并不提供全网的视图。提供必要的信息来构建一个完整的、

一致的、全网的视图，应当作为路由器和交换机的一个主要功能。

3) 直接控制：直接控制意味着控制和管理系统应当能够设置数据平面的状态。在现有典型的 IP 网络中，一个管理域的控制策略是由多个间接控制机制合成的，这种间接合成后的结果不但难以预测，而且还增加了网络控制的复杂性。在直接控制中，决策元负责产生每个交换机的所有状态，由于做出决策控制的算法不在各交换机内运行，因此大大简化了交换机的功能，交换机实现的唯一分布式功能就是邻居发现，并实现决策单元和交换机之间的交互通信，这样交换机内的软件就是轻量级的。

3.3 4D模型

(1) 网络结构图

4D 网络主要由三种设备组成，终端计算机、交换单元以及决策单元（Decision Element）。如图 2 所示。通常，网络中部署多个 DE，但是只有一个主要的 DE 负责配置网络交换机。每个备份的 DE 都会收到相同的来自于交换机的信息，执行与主 DE 相同的计算，但是，备份 DE 不会把它们的计算结果发出去。主 DE 的选择可以是指定的，也可以使用 LE（Leader Election）协议，选择出网络中优先权最高的 DE 作为主 DE。

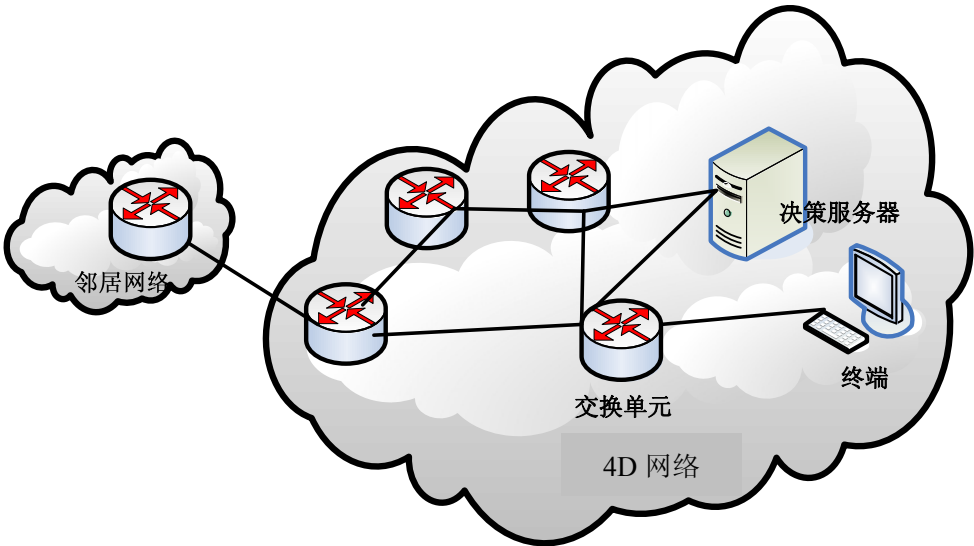


图 2 4D 网络结构图

(2) 四个功能平面

4D 模型将现有网络的网络控制功能所化分的三个平面经过重新整合后，划分为以下四个平面：决策平面（Decision plane）、分发平面（Dissemination plane）、发现平面（Discovery plane）和数据平面（Data plane），如图 3 所示。模型的设计充分体现了上述三个原则，决策平面逻辑实现的基础是全网视图的拓扑结构和流量，由发现平面来收集度量数据，满足网络的目标。决策平面直接控制数据平面的操作，排除建模和转换控制行为的需要。将多数的控制状态和逻辑从路由器中分离出来，简化了数据传送协议，使其不需要嵌入决策逻辑。

网络控制，例如可达性、负载平衡、接入控制以及安全性。决策平面替代原有的管理平面，使用分布式算法来将网络目标直接转化为包处理状态，分别配置到数据平面的交换机/路由器中（例如，转发表条目，包过滤器，查询参数）。

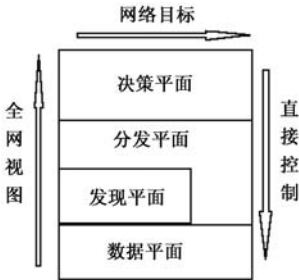


图 3 新的网络功能平面的划分

1) 决策平面：如图 4 所示，决策平面由逻辑上独立的决策单元（简称 DE）或决策服务器组成，DE 使用发现平面收集的信息，做出决策进行

2) 分发平面：如图 5 所示，分发平面负责维护鲁棒的逻辑通路，在决策单元和网络交换机之间

传送控制信息。在数据平面，控制信息可能会与用户信息经过相同的物理链路，但在逻辑上是相互独立的信道。相比而言，在现有的网络中，需要事先通过路由协议为控制信息建立路径。分发平面将决策平面产生的管理信息发送至数据平面，并将发现平面确定的状态发送给决策平面，分发平面自身并不产生任何状态。

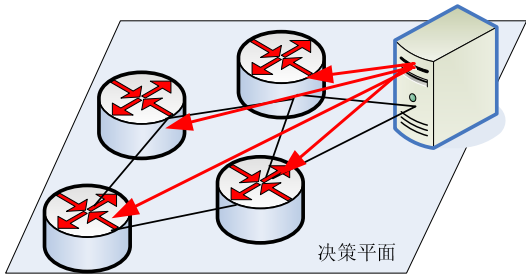


图 4 决策平面

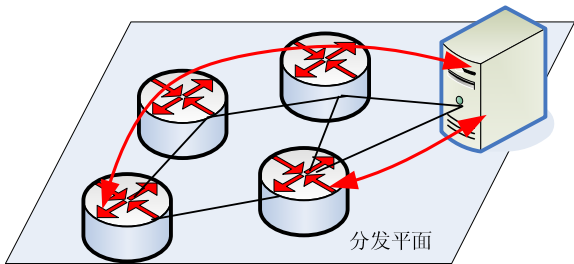


图 5 分发平面

3) 发现平面：如图 6 所示，发现平面负责发现网络中的物理元素，并产生逻辑标识符来描述它们。而现有的 IP 网络，仅能实现两个预先配置好

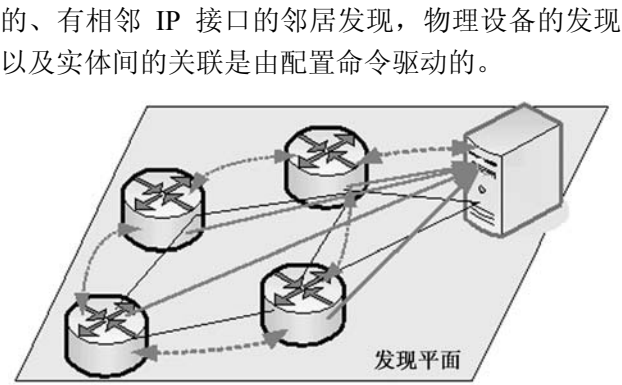


图 6 发现平面

4) 数据平面：如图 7 所示，数据平面位于网络中的交换机（或路由器）组成，它提供用户信息的传送服务，例如 IPv4, IPv6 或以太网数据包转发。数据平面的行为依赖于交换机的状态，这些状态仅由决策平面进行控制。交换机的状态包括：转发表或转发信息库（FIB），队列管理参数，网络地址转换映射等等。

3.4 4D模型的优点

4D 模型与现有的三个功能平面划分模型相比，具有以下几个优点。

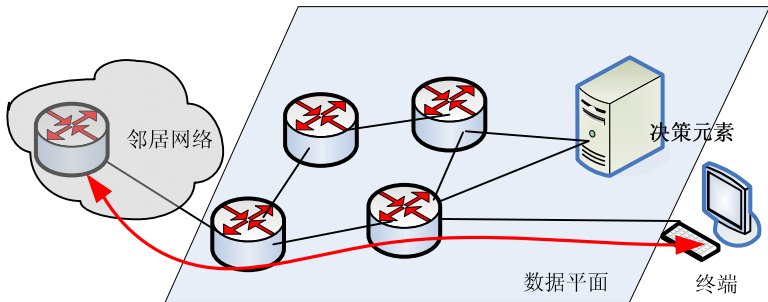


图 7 数据平面

1) 更高的鲁棒性：通过简化网络控制的状态和逻辑，确保底层交换设备（网元）状态的内部一致性，大大地降低了网络的脆弱性。4D 模型为管理网络增加了抽象层，允许网络管理员集中于指定网络目标而不是为每个路由器/交换机配置特殊的协议和机制。全网视图为管理员和网管系统提供了一种新的管理方式，不再需要考虑路由器/交换机

复杂的协议接口。将状态和逻辑从网元移出也产生了新的，灵巧的算法来计算数据平面状态，易于维护和扩展。

2) 更好的安全性：安全性是网络固有的目标。通过在边界路由器安装包过滤，使得决策平面能够更好地保护网络边界。从全网的管理目标出发制定相应的安全策略，而不是依靠逐个路由器的配

置,降低了因配置错误导致的安全威胁的可能性。

3) 适应异构性: 相同的 4D 结构可以用于不同的网络环境,但是需要定制各自的方案。例如,一个 ISP 骨干网有很多优化的标准和高可靠性的需求,决策平面可能由部署于不同区域的多个高端服务器组成。一个带有以太网交换机的数据中心环境可能仅需要一些廉价的计算机,但仍可以比现有的扩展树或静态 VLAN 配置提供更复杂的能力(例如带有弹性的流量工程)。

4) 适应革新以及网络进化: 将网络控制从路由器/交换机和协议中分离出来是很有必要的。决策平面能够融合新的算法,通过计算数据平面状态来满足各类网络目标,而不需要改变数据包格式或控制协议。另外,将控制功能移出路由器/交换机

软件可以由研究机构或第三方软件开发商来设计这些算法。

## 4 结束语

以 4D 模型为代表的革命式发展路线的研究还处于摸索阶段,只是就下一代网络体系结构在理论与应用的某个局部目标展开,没有形成完整的体系,十分缺乏原创性的基础理论和应用技术支持,存在着巨大的创新空间,这为我们在理论技术与应用上取得一批原创性和突破性研究成果提供了很好的机遇。

## 参考文献

- [1] Albert Greenberg, Gisli Hjalmtysson, David A. Maltz, Andy Myers, Jennifer Rexford, Geoffrey Xie, Hong Yan, Jibin Zhan, Hui Zhang. A Clean Slate 4D Approach to Network Control and Management. In ACM SIGCOMM Computer Communication Review. 35 (5). October, 2005.
- [2] Hong Yan, David A. Maltz, T. S. Eugene Ng, Hemant Gogineni, Hui Zhang, Zheng Cai. Tesseract: A 4D Network Control Plane. Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI '07), April 2007.
- [3] Ambient Network Project, <http://www.ambient-networks.org/>
- [4] GENI, <http://www.geni.net>
- [5] T. V. Lakshman, The SoftRouter Architecture, HotNets 2004.
- [6] J. Rexford, etl. al., Network Wide Decision Making: Toward A Wafer Thin Control Plane, HotNets 2004.

## 作者联系方式

通信地址: 北京市丰台区大成路 13 号 A00

邮政编码: 100039

联系电话: 66820269-872 13793231439

# 突发波形在 3G 短波通信中的应用研究

刘振浩 胡中豫 韩艳

**摘 要：**简要介绍了 3G 短波通信的特点及物理层突发波形的结构组成。参考 3G 短波通信标准，设计了物理层突发波形的发送和接收方案，并重点对 BW0 波形中的关键技术进行了研究。采用相关搜索、FFT 捕获的方式实现接收伪随机码的捕获，采用滑动相关方式实现位同步和信道估计。系统在硬件平台上进行了实现，通过整机联试，基本达到了军标要求。

**关键词：**突发波形；3G 短波通信；相关搜索；滑动相关；位同步

## 引言

由于短波通信具有通信距离远、设备简单、开设方便以及战时不易被摧毁等诸多优点，因此在通信领域尤其是军事通信中得到了广泛的应用<sup>[1]</sup>。从八十年代起，二代（2G）短波通信技术为建立远距离和可实现移动话音传输的短波通信网提供了强健可靠的技术系统。2G 短波通信系统采用异步工作方式，支持小规模网络，建链速度慢，自适应通信系统在链路建立、数据传输、组网能力等方面具有一定的局限性。从九十年代中后期开始，随着短波通信网络的不断增加，短波频谱资源日益贫乏，迫切需要新的短波通信技术体制来满足现有短波通信需求。于是，近几年基于 MTL-STD-188-141B 的第三代短波通信系统应运而生。在全面支持第二代协议规定的语音通信和小型网络的前提下，3G 短波通信系统针对目前短波通信中存在的问题，采用呼叫信道同步搜索、载波监听以及突发波形传输等先进技术，在自动链路沟通、网络管理和流量控制等方面取得了重大进展，可有效地支持大规模、数据密集型的短波通信。

3G 短波通信技术体制的一个重要目标就是有效支持由大量站点组成的对等网的突发数据通信。采用了 5 种突发波形传输技术的 3G 短波通信系

统，链路建立最快可达到 1.6s，一次成功建立链路仅需完成双向传输，大大减少了建链时间及 ALE 信息在空中暴露的时间。具有可靠的极低速建链能力和最低限度通信能力，提高了系统最低限度通信的数据包正确接受率可以达到 95%<sup>[3]</sup>，并且具有抗连续波、抗突发干扰能力；全网络步工作，可支持多达 1920 个站点的大信息量工作，有优先级信道访问和防碰撞措施；支持 Internet 协议及应用。本文主要对 3G 短波通信系统中采用的 5 种突发波形（BW0、BW1、BW2、BW3 和 BW4）进行了介绍，重点对 BW0 波形关键技术进行了研究，提出了物理层的设计方案，并在硬件完成了实现。通过硬件联调测试，基本达到了设计要求。

## 1 突发波形结构及特性

应用于 3G-ALE 和数据传输的 5 种突发波形统一采用 8PSK 调制，载波频率为 1800Hz，码元速率 2400B，不同用途的波形对应不同的信号格式。BW0、BW1、BW2、BW3 和 BW4 的波形结构如图 1 所示。其中前导序列用于发方电台的传输等级控制过程和收方电台的自动增益控制过程，探测报头相互正交，用于信号的同步和不同波形的判决。

BW0	前导序列（265个伪随机码）	探测报头（384个伪随机码）	26比特数据
BW1	前导序列（256个伪随机码）	探测报头（576个伪随机码）	48比特数据
BW2	前导序列	探测报头（64个伪随机码）	26比特数据
BW3	前导序列（640个伪随机码）	8*11+25比特数据   CRC校验比特	
BW4	前导序列（265个伪随机码）	2比特数据	

图 1 突发波形（BW）的结构

采用 5 种突发波形进行数据传输的 3G 短波通信系统，可实现短波电台的自动选频和建链，并根据

信道质量估值采用高速或低速数据链路协议来实现数传功能，在链路质量好的情况下选择高速数据

链路协议，在链路质量稍差的情况下选择低速数据链路协议，从而提高了系统的灵活性和数据传输的可靠性。

3G-ALE 协议中的 BW0 PDU（协议数据单元）负责自动链路建立，BW1 PDU 负责进行业务管理和高速数据链路协议的拆链，BW2 PDU 负责高速数据传输，BW3 PDU 负责低速数据传输，BW4 PDU 负责低速数据链路协议的拆链。BW0、BW1 的前导序列用于信号的捕获、伪码的初同步；各自探测报头通过与接收序列进行相关计算可实现位同步、信道估计、突发波形形式的判别；其中 BW0 的探测报头还可用于信道质量分析。在数据接收端将实现了位同步并校正了频差的信息序列进行相关解扩即可恢复出信息。

2 物理层方案设计

3G 短波通信建链时，呼叫方通过调用 BW0 的 ALE PDU 发出建链请求，被呼方根据得出的信道估值确定采取何种数据链路协议进行数传，并告知呼叫方，然后调用 HDL 或 LDL PDU 开始进行数据传输。

链路建立过程中，不同的功能由不同的突发波

形实现，接收端要对突发波形形式进行判别。协议为不同的突发波形提供了各自的探测报头，不同的探测报头之间近似正交。将接收序列与正交的探测报头进行相关计算可以确定突发波形形式。

下面对其中的 BW0 进行介绍。BW0 用于 3G-ALE 链路的建立，传递所有的 3G-ALE PDU（协议数据单元），长度为 1472 个 PSK 码元，持续时间为 613.333ms，由 TLC/AGC 段、探测报头段和数据段组成，其结构和时序如图 2 所示。有效载荷为 26 比特数据信息[2]。



图 2 BW0 结构和时序

26 比特数据信息经过卷积编码生成 52 比特的编码，经过交织和正交符号映射后，形成长度为  $13 \times 16 \times 4 = 832$  的三比特数据符号序列。由 TLC/ACC 保护序列、探测报头序列和数据符号序列组成的信道符号序列以 2400 符号/秒的速率对 1800Hz 的载波进行 8PSK 调制，产生发送波形。其流程图如图 3 所示。

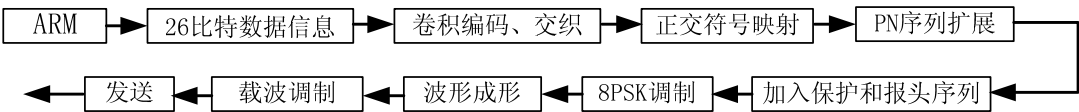


图 3 BW0 发送波形形成过程流程图

2.1 BW0 TLC/AGC 保护序列

BW0 波形中的 TLC/AGC 保护序列是一个长度为 256 的伪随机三比特符号序列[2]，用于发方电台的传输等级控制过程和收方电台的自动增益控制过程，目的是使 TLC 和 AGC 在接收 BW0 探测报头前达到稳定，最小化这些过程对 BW0 探测报头造成的失真。

2.2 BW0 探测报头

BW0 探测报头用于收端检测 BW0 信号、自适应均衡和频偏校正，包含 384 个伪随机三比特符号[2]。

2.3 BW0 数据波形形成

BW0 携带 26 个协议比特有效载荷。经过  $r=1/2$ 、 $k=7$  的卷积编码器，生成 52 比特的编码。编码多项式如下：

$$b0 = \text{input} + X^6 + X^4 + X^3 + X^1 + 1 \tag{1}$$

$$b1 = \text{input} + X^6 + X^5 + X^4 + X^3 + 1 \tag{2}$$

编码后的序列使用  $4 \times 13$  矩阵进行交织。输入为 52 比特数据，输出为 13 个 4 比特序列，4 比特序列用于正交符号映射。交织器每次从交织矩阵中取出一个 4 比特序列，按照 3G 短波通信协议标准中 BW0 的正交符号映射表[2]将其映射成 16 个三比特符号序列，重复冗余 3 次，得到长度为 64 的三比特符号序列。经过编码、交织和正交符号映射

后, 26 比特有效载荷形成长度为  $13 \times 16 \times 4 = 832$  的三比特符号序列。

根据 BW0 波形的 PN 表生成的 832 个三比特伪随机序列与与前述正交符号映射形成的 832 个三比特符号做模 8 加得到 832 个三比特符号数据序列。

## 2.4 BW0 调制

BW0 波形信道符号序列由 256 个三比特

符号的 TLC/ACC 保护序列、384 个三比特符号的探测报头序列和 832 个三比特符号数据序列组成。信道符号序列生成后, 以 12KHz 的采样频率进行采样, 码元速率为 2400 码元 / s, 每个码元采 5 个样点, 中间的样点是最佳采样时刻。采样后的数据经过升余弦滤波器进行波形成型, 然后调制到 1800 Hz 的副载波上, 按图 4 所示产生发送波形进行发送。BW0 波形经过调制后生成的发送波形如图 5 所示。

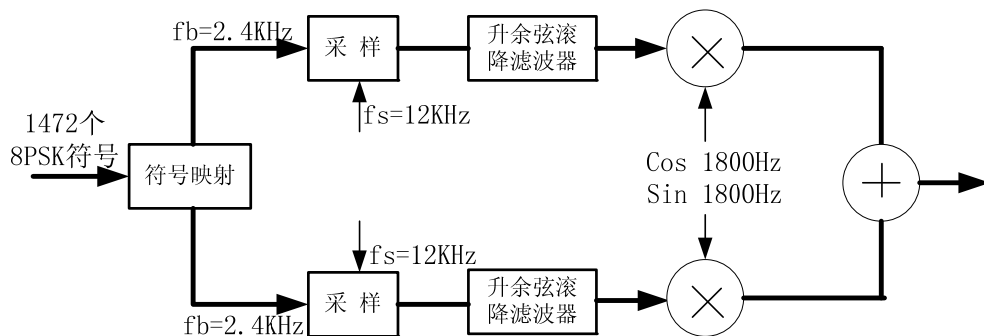


图4 载波调制框图

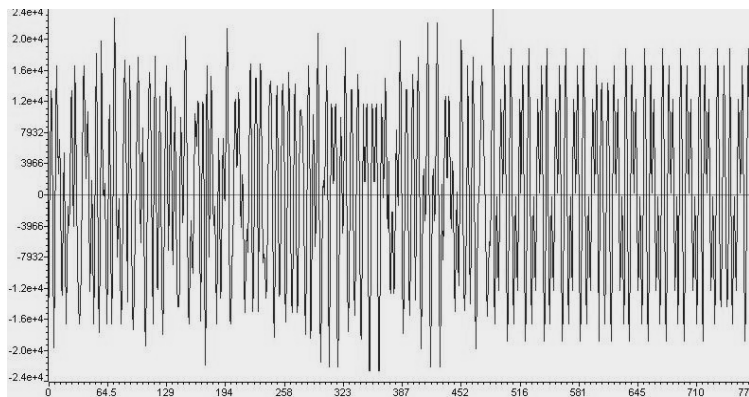


图5 BW0调制后的发送波形

## 3 关键技术及硬件实现

接收机要从接收信号中恢复出所传输的信息, 首先要对接收信号进行相关解扩; 而接收信号正确的相关解扩是建立在与接收信道伪随机符号精确同步的基础上的。同步分为初同步<sup>[4][5]</sup> (又称为伪随机码的捕获) 和精细同步<sup>[4][5]</sup> (又称位同步) 两个阶段。

### 3.1 伪随机码的捕获

本方案采用相关搜索、FFT 捕获的方式

实现接收伪随机码的捕获。令接收信号  $r(t)$  的载波频率为  $f_l$ , 相位为  $\phi_k$ ,  $c(t)$  是幅度受到伪随机序列调制的 8PSK 调制信号, 对接收信号以  $f_s = 12\text{kHz}$  的采样频率进行采样后可表示为:

$$r(kT_s) = c(kT_s) e^{j(2\pi f_l kT_s + \phi_k)} \quad (3)$$

由于短波信道中存在着多普勒频移, 导致系统收发双方存在频差  $f_d$ , 接收信号解调、滤波后的表达式为:

$$r(kT_s) = c(kT_s) e^{j(2\pi f_d T_s + \phi_k)} \quad (4)$$

将解调后的每个码元取一个点与本地序列信号



的共轭复数进行滑动相乘, 相乘后信号可表示为:

$$p(kT_c) = c(kT_c) \overline{c((k+n)T_c)} e^{j(2\pi f_d T_c + \phi_k)} \quad (5)$$

式中  $T_c$  为码元周期,  $T_c = 5 \times T_s$ 。当接收信号与本地序列信号的相位差  $n \neq 0$  时, 相乘后得到的信号是随机信号序列, 对该信号做 FFT 变换不会出现明显的谱峰。当  $n$  为 0 时, 即本地序列信号与伪随机码同步时,

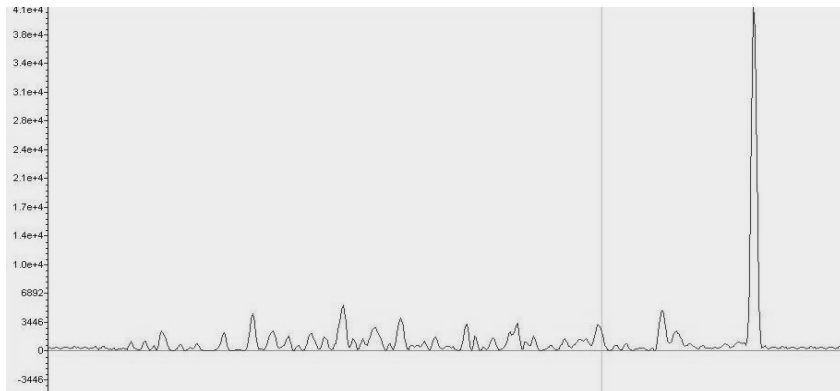


图6 捕获到接收信号时的谱峰波形

由于噪声影响, 可能会产生伪码的假同步, 因此要进行捕获确认。在第一次 FFT 峰值大于门限值时, 记录峰值所在那一段的段号和峰值出现的位置 (即频差)。然后再做三次确认, 每次接收十个样点, 接收序列窗口移动十点, 从那段起始位置开始向后移动两个码元, 与本地序列信号相乘, 积序列作 265 点 FFT。分别找出三次 FFT 的最大值及其出现位置, 若其中至少有两次峰值超过了门限且两次峰值出现位置与第一次峰值出现位置相互之间的差值都小于一定范围, 则认为已正确捕获并求得频差。否则重新开始搜索。

由于 FFT 对位同步不敏感, 因此无法用谱峰对应的时域位置作为位同步, 但在这个位置和真正的位同步位置相差在一个码元之内, 所以可以用作初步的位同步结果, 接下来的工作就是校正频差后通过相关完成位同步。

### 3.2 位同步与信道估计

方案中的位同步目的是要准确地找到码元中点的位置。在捕获的同时已经获得了初步的位同步信息, 此时的位同步位置与真正的码元中点相差不到一个码元。

由于相关对位同步位置较为敏感, 所以将校正频差后的接收序列与本地序列进行滑动相关, 在初

$p(kT_c)$  可表示为:

$$p(kT_c) = e^{j(2\pi f_d T_c + \phi_k)} \quad (6)$$

对该信号做 FFT 变换, 在对应频率为  $f_d$  的位置处会出现明显谱峰, 硬件上验证结果如图 6 所示。当功率谱中相应位置出现明显谱峰时, 就可以认为已捕获到信号, 同时根据谱峰位置计算出接收信号的频率或系统的频差。

步位同步位置左右两侧一个码元之内寻找最大的相关峰, 即可获得码元中点的准确位置。

在 BW0 波形成形过程中, 每个码元的 5 个样点中只有中间的样点码间干扰最小, 因此找到码元的最佳抽样点即可实现位同步。由于短波信道存在多径和衰落的干扰, 还必须通过信道估计找到主径和多径信号的位置。

BW0 波形采用的码元速率为 2400 符号/s, 每个码元宽度大约为 0.42ms, 3G 短波通信协议中给出的短波信道多径时延在 0.5~2ms, 大于一个码元的宽度, 在理论上可将多径和主径分离。以 12KHz 的采样速率, 2ms 内对应 24 个采样点, 考虑到多径时延的不确定性, 以初始同步位置为中心对前后 30 个样点进行滑动相关计算, 共得出 61 个相关值。在中心位置前后 1 个码元 (5 个样点) 的范围内观察相关峰的位置, 以此来确定主径的位置 (即最佳抽样时刻)。由于多径信号也携带信号信息, 所以与本地序列相关后会在多径位置出现一个相关峰。因此, 可以在一次滑动相关的过程中来确定主径和多径的位置。

### 3.3 解扩、解交织和译码

在获得了所有同步信息后, 对接收信号进行相关解扩。通过采用 Rake 接收技术实现多径分集,



可大大提高抗干扰和抗衰落性能。本方案采用分集接收,通过滑动相关将主径和多径分离,并通过恰当合并,获得最大的输出信噪比。将解扩后的数据进行解交织和 Viterbi 译码,恢复出原始信息。由于解交织和 Viterbi 译码技术相对简单,在此就不再赘述。

### 3.4 硬件实现

系统硬件实现平台如图 7 所示。系统采用

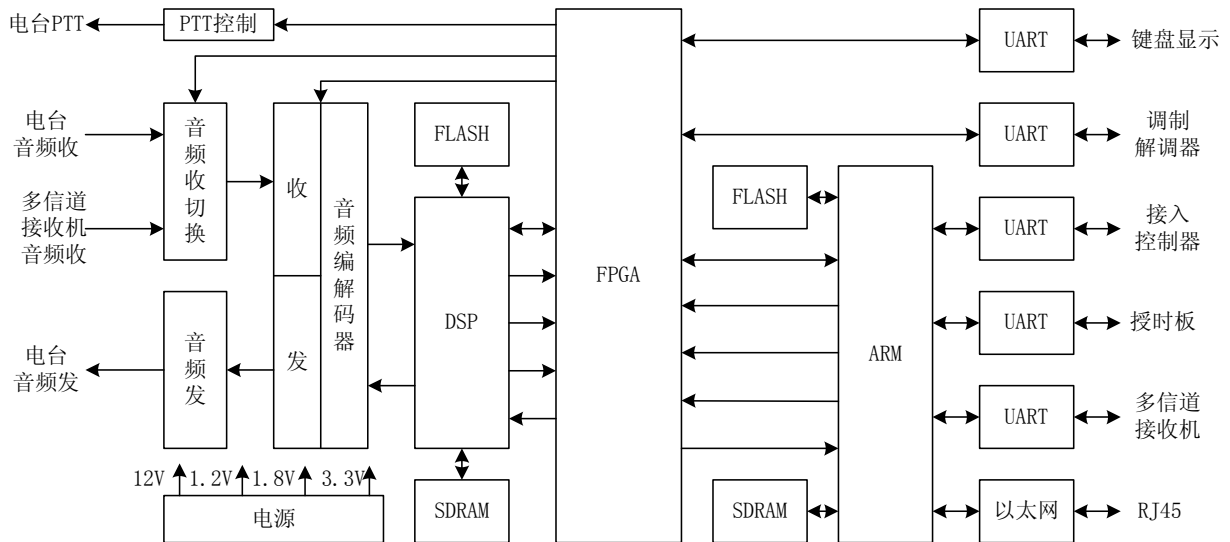


图 7 3G 短波通信硬件系统结构

## 4 结束语

本文参考 3G 短波通信协议标准（如 MIL-STD-188-141B），根据突发波形结构及短波信道特点，完成了 3G 短波通信物理层方案设计，对关键技术进行了算法研究，并在硬件平台上实现了

ARM、DSP 和 FPGA 及外围设备共同完成。DSP 主要完成整个通信系统的协调工作和通信协议的实现。FPGA 主要完成 BW0 波形的调制、解调、信号编解码、交织、解交织等工作。ARM 主要用来完成对整个系统的控制功能。通过 RS232 与 ARM 相连的以太网口可实现对整个系统的远程控制和系统应用程序的升级，大大提高了系统功能的灵活性。

BW0 波形的发射和正确接收。需要指出的是，由于短波信道的多径效应、时变特性等因素引起的码间干扰对高速数据通信影响很大，为提高 3G 短波数据通信的可靠性和有效性，采用高性能的自适应均衡技术尤为必要。

### 参考文献（略）

- [1] 胡中豫, 现代短波通信, 国防工业出版社, 2003
- [2] U.S.MIL-STD-188-141B\_C:THIRD-GENERATION HF LINK AUTOMATION
- [3] 薛松, 崔恩吉, 短波通信技术发展与分析, 通信与广播电视.2004 (4)
- [4] 张文泉, 第三代短波通信系统物理层研究与 DSP 实现.广东通信技术, 2005.11
- [5] 冯子龙, 第三代短波链路自动建立技术研究.硕士研究生毕业论文.2003.01
- [6] Eric E.Johnson, Simulation results of Third Generation HF Automatic Link Establishment.Processing of MILCOM'99, 1999

### 作者联系方式

通信地址: 重庆通信学院科研所

邮政编码: 400035

联系电话: 13883955749 023-68759473

# 飞秒脉冲在光子晶体光纤中的传输特性分析

雒开彬 车雅良 何小梅

**摘要:** 基于广义非线性薛定谔方程, 利用分步傅立叶法数值模拟了高斯飞秒脉冲在光子晶体光纤中的传输特性。结果表明: 高斯脉冲在很短距离内形成孤子衰变, 频谱红移显著; 另外, 三阶色散会导致脉冲波形及频谱不对称, 出现精细结构, 并且有形成孤子的趋势; 脉冲内拉曼散射对脉冲有平滑作用; 自陡展宽了蓝侧部分, 有部分能量转移到蓝移分量。

**关键词:** 飞秒脉冲; 光子晶体光纤; 孤子衰变; 孤子自频移

光子晶体(PC)是一种介电常数随空间结构周期性变化的新型光学微结构材料, 其概念是1987年分别由 S. John 和 E. Yablonovitch 提出<sup>[1]</sup>。光子晶体光纤(PCF)是空气洞呈周期性排列、并利用光子带隙效应或改进的全内反射效应传导光的光纤, 与传统光纤不同, PCF 是由其中周期性排列空气孔的单一石英材料构成的, 因此又被称为多孔光纤(holey fiber)或微结构光纤(micro-structured fiber)。这种光纤中, 折射率在垂直于光纤轴向的剖面的两维都是周期性的, 而在传播方向上没有周期性。PCF 自 1996 年问世以来<sup>[2]</sup>, 在实验和理论研究上吸引了众多研究者的注意<sup>[2~4]</sup>。

由于 PCF 是由一种材料拉制而成, 不存在不同热膨胀系数的两种类型玻璃的边界问题, 可以推测其最终损耗值会远远低于传统光纤<sup>[5]</sup>; 具有良好的色散特性, 可以在很宽的波长范围内得到较大的色散, 在可见波段具有零色散点甚至能够出现负色散, 并且其零色散点可调, 只需改变 PCF 的尺寸, 就可以在几百 nm 的范围内取得零色散; 另外, 在增大光纤纤芯和包层的折射率差可以提高光场局部集中程度, 从而提高光学非线性作用的效率。这些都满足了产生超连续谱的色散和非线性要求, 因此光子晶体光纤被广泛的用于产生超连续谱。超连续谱对于超短脉冲的产生、光学频率测量、光学相干层析等许多应用都有重要的意义。

在实际应用中, 由于许多激光器发射的脉冲都近似为高斯形, 因此研究这种类型的飞秒脉冲在光子晶体光纤中传输特性, 更加具有现实指导意义。研究发现, 由于高斯飞秒脉冲传输时, 在光纤内同时存在自相位调制和其他非线性效应, 如脉冲内拉曼散射、自陡效应等, 都会影响飞秒脉冲的非线性

传输以及超连续谱的产生。本文基于非线性薛定谔方程, 从理论上研究了飞秒脉冲的传输特性, 并得出一些初步结论。

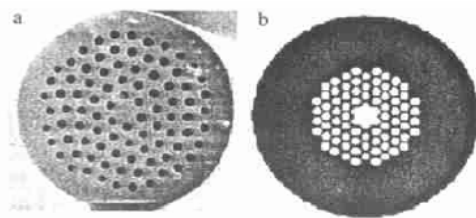


图1 光子晶体光纤横截面图

## 1 理论模型

光子晶体光纤中脉冲的传输可以用广义非线性薛定谔方程描述:

$$\frac{\partial A}{\partial z} = -i \frac{\beta_2}{2} \frac{\partial^2 A}{\partial T^2} + \frac{\beta_3}{6} \frac{\partial^3 A}{\partial T^3} - \frac{\alpha}{2} A + i \gamma \left( |A|^2 A + i \frac{1}{\omega_0} \frac{\partial (|A|^2 A)}{\partial T} - T_R A \frac{\partial |A|^2}{\partial T} \right)$$

其中,  $A$  为脉冲包络的慢变振幅,  $T = t - z/v_g$ ,  $\beta_2$  为 GVD 参量,  $\beta_3$  为 TOD 参量,  $\alpha$  代表光纤损耗,  $\gamma$  为非线性系数,  $\gamma = \frac{n_2 \omega_0}{c A_{\text{eff}}}$ ,  $n_2$  为非线性折射率,  $A_{\text{eff}}$  为有效纤芯截面,  $T_R$  为非线性响应函数的一阶矩,  $T_R = f_R \int_{-\infty}^{\infty} t^* h_R(t) dt$ ,  $f_R$  表示延时拉曼响应对非线性极化的贡献,  $h_R(t)$  为拉曼响应函数。方程右端前两项描述群速度色散(GVD)和三阶色散(TOD), 第三项表征光纤损耗, 后三项分别为自相位调制(SPM)、自变陡(SST)以及

脉冲内拉曼散射 (SRS)。

具有初始啁啾的高斯脉冲形式为:

$$A(0, T) = \sqrt{P_0} \exp \left[ -\frac{1 + iC}{2} \frac{T^2}{T_0^2} \right]$$

由于方程 (1) 没有解析解, 一般采用数值计算。常用的方法为分步傅立叶算法<sup>[6]</sup>:

$$\frac{\partial A}{\partial z} = (\hat{D} + \hat{N})A$$

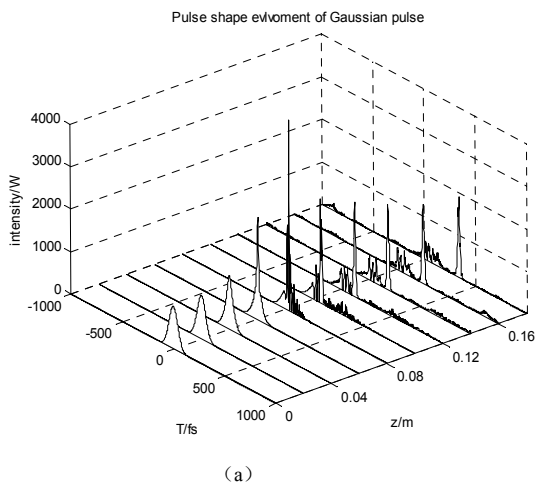
其中,  $\hat{D}$  为差分算符, 表示色散和吸收;  $\hat{N}$  为非线性算符, 描述脉冲在光纤中传输的非线性效应。

$$\hat{D} = -i \frac{\beta_2}{2} \frac{\partial^2}{\partial T^2} + \frac{\beta_3}{6} \frac{\partial^3}{\partial T^3} - \frac{\alpha}{2}$$

$$\hat{N} = i\gamma \left( |A|^2 + i \frac{1}{\omega_0 A} \frac{\partial (|A|^2 A)}{\partial T} - T_R \frac{\partial |A|^2}{\partial T} \right)$$

## 2 数值计算结果及分析

模拟初始脉宽为 100 fs (脉冲 1/e 处宽度  $T_0=60$  fs), 中心波长为 800 nm, 峰值功率为 1kw



的高斯脉冲在 PCF (忽略损耗) 中的传输特性。

选用直径  $2\mu\text{m}$  的 PCF (零色散波长 767 nm), 其参数为: 非线性系数  $\gamma=75/\text{Wkm}$ , 800 nm 处 GVD 参量  $\beta_2=-6\text{ps}^2/\text{km}$ , TOD 参量  $\beta_3=6.05 \times 10^{-2}\text{ps}^3/\text{km}$ ,  $T_R=1.44\text{fs}$ 。  $L_D = \frac{T_0^2}{|\beta_2|} = 0.6\text{m}$ ,

$$L_D = \frac{T_0^3}{|\beta_3|} = 3.6\text{m}, \quad L_{NL} = \frac{1}{\gamma P_0} = 0.013\text{m}。$$

### 2.1 数值模拟无啁啾高斯脉冲的传输特性

从图 2 中可以看出, 在色散与 SPM 的作用下, 高斯脉冲后沿很快发生畸变, 形成非对称的较深调制的振荡结构, 由于自陡效应与脉冲内拉曼散射, 峰值位置向后沿移动, 脉冲出现分裂, 随着传输距离进一步增加, 明显分离, 导致孤子衰变。这是由于孤子谱峰产生红移导致群速度减小造成的。

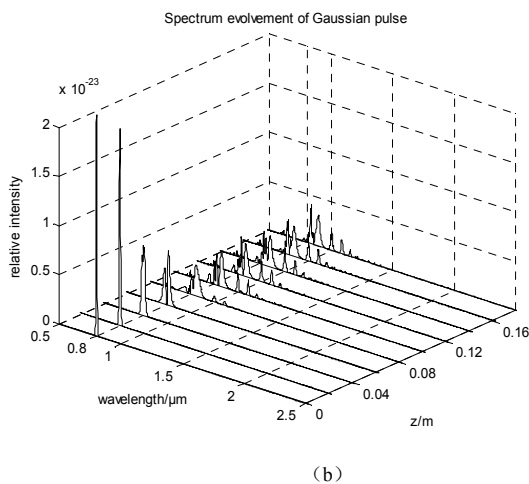
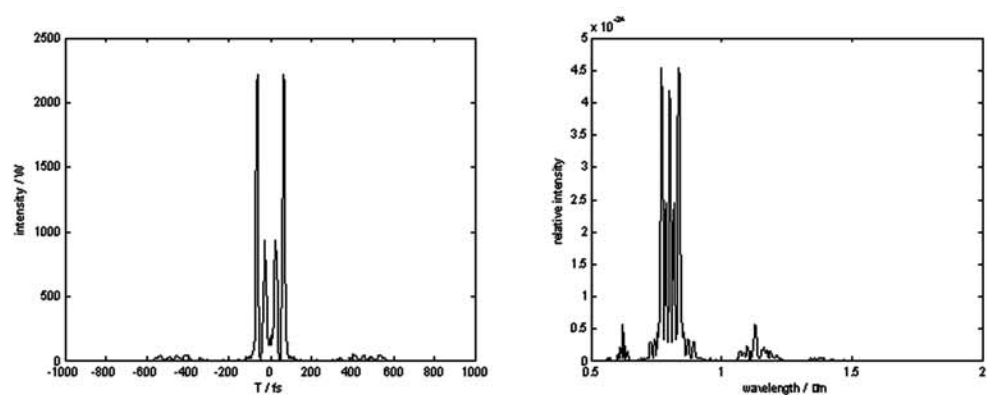


图2 无啁啾高斯脉冲的波形 (左) 和频谱 (右) 演变图 (峰值功率 1kw)

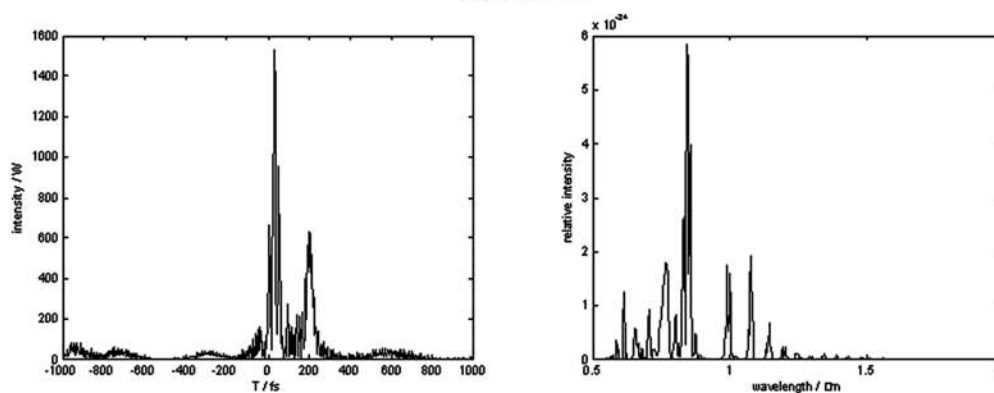
高斯脉冲频谱红移显著, 逐渐展宽, 表现为孤子自频移。由于在反常色散区, 蓝移分量要比红移分量传输的快, 蓝移分量超前, 因此, 红移较宽的谱峰对应图 2 (a) 中右侧的强孤子, 蓝移的谱对应左侧的峰。对于谱宽非常宽的脉冲, 其蓝移谱分量作为泵浦, 通过拉曼增益对相同脉冲的红移分量有效放大, 使得能量从蓝移分量转移到红移分量。

### 2.2 不同效应对传输的影响

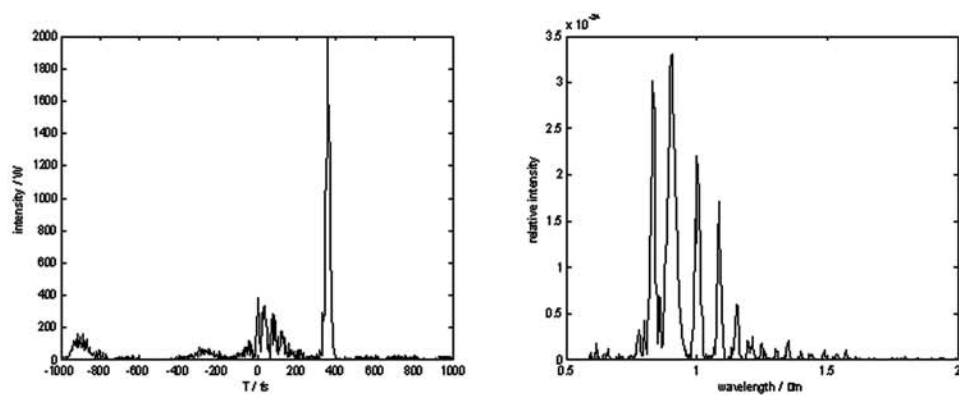
为了更清晰地了解脉冲波形及频谱演变过程中的物理机制, 分别计算了同一功率条件下, 脉冲在光子晶体光纤中传输时不同因素的作用结果, 如图 3。



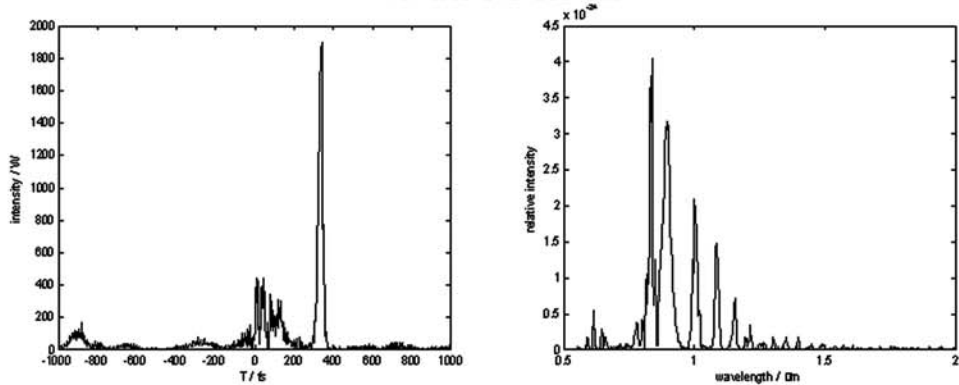
(a) SPM+GVD



(b) SPM+GVD+TOD



(c) SPM+GVD+TOD+SRS



(d) SPM+GVD+TOD+SRS+SST

图3 同一功率条件(1kw)下,不同因素对脉冲和频谱的影响

(图 a): 仅有自相位调制 (SPM) 和群速度色散 (GVD) 时, 高斯脉冲的时域波形和频谱均为多峰对称结构 (以频率为横轴变量时, 频谱对称), 这是由于在 SPM 作用下, 高斯脉冲前沿红移, 后沿蓝移, 而中心部分频率啁啾几乎为零, 而在负色散光纤中, 蓝移分量的速度要大于红移分量, 因此, 脉冲不同频谱分量速度不同而造成了脉冲分裂, 形成如图所示的多峰结构, 虽然此时

$$N^2 = \frac{L_D}{L_{NL}} \gg 1, \text{ GVD 也不能作微扰处理, 因为}$$

大量的 SPM 所致啁啾作用于脉冲, 即使是较弱的色散效应也会引起脉冲显著变形; GVD 与 SPM 共同引入的非线性啁啾使的脉冲相位变化剧烈, 从而造成频谱的振荡。(图 b) TOD 的引入使得脉冲波形与频谱严重不对称, 形成复杂的振荡结构, 脉冲开始分裂, 有形成孤子的趋势, 实际上, 如果只有 TOD 单独作用时, TOD 自身也会导致孤子衰变<sup>[8]</sup>。

(图 c) 脉冲内拉曼散射使频谱发生显著红移, 蓝

移分量所占能量比例很小; 脉冲中的精细结构被削弱, 脉冲变得平滑, 出现了主峰与次峰, 分别对应于频谱的红移分量和蓝移分量。(图 d) 自陡展宽了蓝侧部分, 有部分能量转移到蓝移分量。

### 3 结论

用分步傅立叶法求解非线性薛定谔方程, 模拟了高斯飞秒脉冲在光子晶体光纤中的传输特性, 研究发现, 高斯脉冲在很短距离内形成孤子衰变, 频谱红移显著, 表现为孤子自频移。通过独立分析各个因素的影响, 可以发现, 三阶色散造成脉冲波形与频谱不对称, 有出现孤子的趋势; 脉冲内拉曼散射使脉冲平滑, 红移显著; 自陡展宽了蓝侧, 对脉冲能量重新进行分配。这些结果对于研究超连续谱的产生和应用具有重要意义。

### 参考文献

- [1] E. Yablonovitch. Inhibited spontaneous emission in solid-state physics and electronics. *Phys. Rev. Lett.* 1987, 58 (20) :2059-2062. S.John. Strong localization of photons in certain disordered dielectric superlattices. *Phys. Rev. Lett.* 1987, 58 (23), 2486-2489.
- [2] J.C. Knight, T.A. Birks et al. All-silica single-mode optical fiber with photonic crystal cladding. *Opt.Lett.* 1996, 21 (19) :1547-1549.
- [3] T.A. Birks, J.C. Knight et al. Endlessly single-mode photonic crystal fiber. *Opt.Lett.* 1997, 22 (13) :961-963.
- [4] T.M. Monro, P.J. Bennett et al. Holey fibers with random cladding distributions. *Opt.Lett.* 2000, 25 (4) :206-208.
- [5] M.D. Nielsen, C. Jacobsen et al. Low-loss photonic crystal fibers for transmission systems and their dispersion properties. *Optics Express.* 2004, 12 (7) :1372~1376.
- [6] Govind P. Agrawal. Nonlinear fiber optics[M]. Beijing: Publishing House of Electronics Industry, 2002.
- [7] P.K.A.Wai, C.R.Menyuk, Y.C.Lee, and H.H.Chen. Nonlinear pulse propagation in the neighborhood of the zero-dispersion wavelength of monomode optical fibers. *Opt.Lett.* 1986, 11 (7) :464-466.

### 作者联系方式

通信地址: 西安通信学院基础部计算中心

邮政编码: 710106

联系电话: 13759870660

# 基于视觉注意机制的军事遥感图像ROI提取

马大玮 李晓飞 陈正荣 凤光华

**摘 要：**本文提出了一种基于视觉注意的军事遥感图像感兴趣区域（ROI）提取方法，充分利用了微目标遥感图像的灰度、轮廓、大小等信息特征。该方法采用形态学 Top-Hat 变换强化感兴趣区域和抑制背景，利用开运算实现去除噪声和虚假微目标；通过阈值迭代法初步分割出感兴趣区域；最后结合形态学方法进行感兴趣区域提取；运用基于小波变换的多尺度边缘检测算法探测出感兴趣区域的边界。仿真结果表明该方法能快速有效地分割提取出军事遥感图像的微目标感兴趣区域。

**关键词：**感兴趣区域；视觉注意；遥感图像；数学形态学；小波变换

在远程探测、精确制导、军事侦察等军事信息化建设的许多场合中，高分辨率遥感图像处理的应用是十分普遍的。对于遥感图像中的微小目标的检测提取是高分辨率遥感图像处理的重要研究方向，由于受到背景复杂、目标繁多、灰度变化频繁等因素的影响，目前较为成熟的目标检测方法往往无法很好地提取遥感图像中的微目标，这也使得遥感图像的微目标提取算法研究成为了目标识别和检测领域的热点和难点问题。

科学研究表明人们的视觉系统具有潜在的选择性注意机制，在观察和理解图像时能够不自觉地对某些目标区域产生兴趣；这种机制被称为“视觉注意机制（Visual Attention Mechanisms）”，这些区域被称为“感兴趣区域（Region of Interest）”。从本质上看，视觉注意就是大脑对一定视觉信息的指向和集中<sup>[1]</sup>。当一定空间提示范围出现时，可以利用其对该范围内输入的信息特征，以足够简单的方法检测提取出感兴趣区域，从而能够实现目标的快速有效识别。本文在充分研究利用微目标遥感图像中的灰度特征、轮廓特征、大小特征、位置布局特征等基础上，利用了视觉注意机制，首先采用基于灰度形态 Top-Hat 变换实现背景抑制和强化所要提取的微目标区域，通过灰度形态开运算完成去除噪声和虚假微目标；然后采用阈值迭代法将微目标感兴趣区域初步从背景中分割出来；最后通过人工交互，用形态学方法进行感兴趣区域提取，然后运用基于小波变换的多尺度边缘检测算法探测出感兴趣区域的边界，从而有利于进行进一步的感兴趣区域编码。

## 1 采用形态学进行图像预处理

数学形态学以严格的数学理论和几何学为基础，用具有一定结构和特征的结构元素去探测图像，从中提取需要的信息特征，以达到对图像分析和识别的目的。它与人的视觉特点有着许多相似之处，故结合视觉注意机制，利用形态学运算进行图像预处理可以强化具有特定信息特征的微目标感兴趣区域。

### 1.1 形态学基本运算

考虑到系统运算速度等问题，本文仅选取灰度遥感图像进行处理，下面只给出一些灰度形态学基本运算的定义。假定  $f$  为灰度图像， $B$  为结构元素。

则灰度腐蚀定义为：

$$(f \ominus B)(x, y) = \min\{f(x - i, y - j) - B(i, j)\} \quad (1)$$

灰度膨胀定义为：

$$(f \oplus B)(x, y) = \max\{f(x - i, y - j) + B(i, j)\} \quad (2)$$

度形态开定义为：

$$f \bullet B = (f \ominus B) \oplus B \quad (3)$$

灰度形态闭定义为：

$$f \blacklozenge B = (f \oplus B) \ominus B \quad (4)$$

### 1.2 基于灰度形态Top-Hat变换的背景消除

Top-Hat 变换作为有效的形态变换可以突出较

暗背景中的亮像素点或突出较亮背景中的暗像素点<sup>[2]</sup>。采用 Top-Hat 变换能够很好地结合视觉注意机制,增强灰度图像中的对比度、亮度等细节特征,以达到去除图像的低频背景,保留感兴趣区域的预处理效果。

Top-Hat 算子定义为:

$$h = f - (f \circ B) \quad (5)$$

其对偶算子定义为:

$$h' = (f \bullet B) - f \quad (6)$$

结构元素的选择对于 Top-Hat 变换检测效果的影响很大,采用不同大小的结构元素,检测结果和运算量会有很大不同。由于微目标还是要占几个到十几个像素,有一定的面积,根据 Top-Hat 变换的概念,结构元素要大于或等于微目标的面积,但过大的结构元素往往会保留过多的虚假目标和噪声信号,同时也会增加算法的运算量。本文算法中选择  $10 \times 10$  的方形结构元素对原始图像采用其对偶算子进行 Top-Hat 变换。

### 1.3 基于灰度形态开运算的噪声滤除

灰度形态滤波器在微目标检测中具有很好的效果,这主要是微目标的类脉冲噪声特性和形态滤波器在滤除脉冲噪声和保护图像细节信息方面的优异性能所决定的。这里,我们将灰度形态滤波应用于微目标检测中,提出了一种基于灰度形态开运算的噪声滤除方法,有利于强化得到视觉注意的微目标感兴趣区域。

采用开运算可以消除比背景亮且尺寸比结构元素小的噪声区域<sup>[2]</sup>,从而达到保留感兴趣区域和提高检测效率的目的。所以,这里选择的结构元素应比目标区域小。本文算法中选择  $4 \times 4$  的方形结构元素对图像进行开运算。

## 2 采用阈值迭代法进行图像分割

经过上述预处理过程后得到的图像已经充分突出和加大了感兴趣区域和背景区域之间的亮度、对比度等差别。结合视觉注意的特点,可以充分利用这些反差特征将作为前景的感兴趣区域和背景区域有效的分割开来,因此在这里采用阈值迭代法进行图像分割处理以便完成进一步的感兴趣区域提取。

阈值迭代法等同于数学上的逐步逼近和迭代。

每一幅图像都存在一个最佳的阈值,也就是我们选取阈值的理想值,设为  $T$ ,首先根据某种规则得到图像的一个阈值  $t$ ,然后不断的修正  $t$  直到它无限趋近于  $T$ 。具体步骤如下。

1) 求出图像的最大灰度值和最小灰度值,分别记为  $f_{\max}$  和  $f_{\min}$ ,令初始阈值  $t = (f_{\max} + f_{\min})/2$ ;

2) 根据阈值  $t$  将图像分割为前景和背景,分别求出两者的平均灰度值  $f_1$  和  $f_2$ ;

3) 求出新阈值  $t_0 = (f_1 + f_2)/2$ ;

4) 若  $t_0$  不等于  $t$ ,则把  $t_0$  的值赋给  $t$ ,转到步骤 2),循环迭代计算。直到  $t$  等于  $t_0$ ,则迭代结束,所得  $t$  即为预先假定的最佳阈值  $T$ 。

## 3 采用小波变换进行多尺度边缘检测

经过以上处理完成了初步的图像分割,接下来通过人工交互,采用形态学方法便可以提取出微目标感兴趣区域。最后我们对其运用基于小波变换的多尺度边缘检测算法进行检测,探测出感兴趣区域的边界。

小波变换的多分辨率能力和频带等指数划分特点符合人类的思维方式和生理功能;同时,二维小波变换中的方向选择性也非常适合于人眼的视觉系统特性。因此,采用基于小波变换的多尺度边缘检测可以充分体现人类视觉注意的特性,同时还具有检测局部突变的能力,利用其获取图像的边缘效果较好。

我们将边缘像素最有用的两个特征——灰度的变化率和方向,分别用梯度矢量的模和幅角来表示,则得到了小波变换的模极大值运用于图像边缘检测的算法,具体方法如下:

假定  $\theta(x, y)$  为二维平滑函数,其沿  $x, y$  两个方向的一阶导数分别表示为:

$$\begin{cases} \psi^1(x, y) = \partial\theta(x, y)/\partial x \\ \psi^2(x, y) = \partial\theta(x, y)/\partial y \end{cases} \quad (7)$$

下面定义二维小波变换为:

$$\begin{cases} \psi_s^1(x, y) = \frac{1}{s^2} \psi^1\left(\frac{x}{s}, \frac{y}{s}\right) \\ \psi_s^2(x, y) = \frac{1}{s^2} \psi^2\left(\frac{x}{s}, \frac{y}{s}\right) \end{cases} \quad (8)$$

因此,在尺度  $s$  上  $f$  的二维小波变换含有两个

分量, 即:

$$\begin{cases} W_s^1(x, y) = f * \psi_s^1(x, y) \\ W_s^2(x, y) = f * \psi_s^2(x, y) \end{cases} \quad (9)$$

此时, 梯度矢量的模为:

$$M_s f(x, y) = \sqrt{|W_s^1 f(x, y)|^2 + |W_s^2 f(x, y)|^2} \quad (10)$$

幅角为:

$$A_s f(x, y) = \arctan[W_s^2 f(x, y) / W_s^1 f(x, y)] \quad (11)$$

在由幅角  $A_s f(x, y)$  所决定的方向上, 求出  $M_s f(x, y)$  的局部模极大值, 就得到了固定尺度  $s$  下的边缘点。为了便于计算, 通常取  $s = 2^j, j \in Z$ 。当  $j$  取不同的值, 便可得到多个尺度的边缘点, 对其进行边缘连接匹配构成了  $f$  的精确定位边缘图像。考虑到运算速度以及最高一级小波分解所含边缘点多少的因素, 本文算法中选择  $j = 3$ 。

## 4 仿真实验结果

为了验证本文算法的有效性和提取效果, 选择一幅含有微目标的遥感图像进行实验, 大小为  $128 \times 128$  像素, 如图 1 所示。根据以上提取算法的步骤对原始图像进行处理, 结果图像分别如图 2~图 5 所示。

采用本文算法得到的提取结果表明: 结合视觉注意机制, 利用形态学对原始图像进行预处理很好地强化了作为感兴趣区域的飞机微目标区域, 同时抑制了遥感图像的背景和噪声干扰 (图 2、图 3); 基于阈值迭代法的图像分割在充分利用诸多反差特征的基础上, 将作为前景的感兴趣区域和背景区域有效的分割开来 (图 4); 然后通过人工交互, 采用形态学方法精确地提取出了微目标感兴趣区域 (图 5); 最后采用基于小波变换的多尺度边缘检测方法实现了边缘的快速、准确定位, 同时也保证了边缘的封闭性和连续性, 很好地实现了目标的完全分割 (图 6)。



图 1 原始图像



图 2 形态 Top-Hat 变换



图 3 形态开运算



图 4 阈值迭代分割

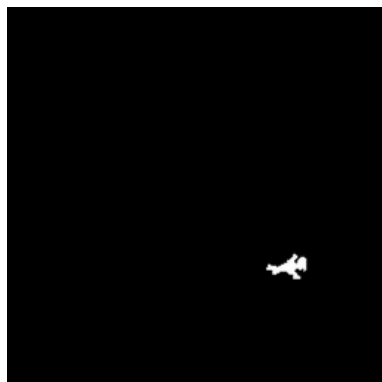


图 5 感兴趣区域提取

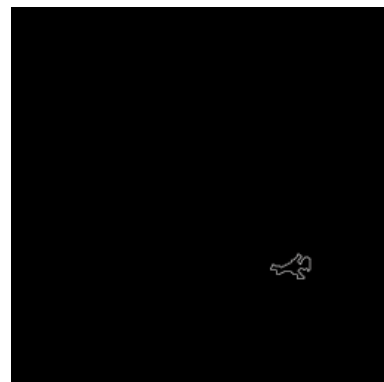


图 6 小波多尺度边缘检测



## 5 结束语

本文提出了一种基于视觉注意的微目标遥感图像感兴趣区域提取方法,有效地实现了对遥感图像微目标的提取,检测出了单像素、闭合的微目标边

缘,为感兴趣区域编码等后续工作提供了很好的数据特征,为在远程探测、精确制导、军事侦察等领域中进行遥感图像相关处理,提供了一定的参考和实用价值。

## 参考文献

- [1] Posner MI. Orientation of attention[J]. Quart Journal of Experimental Psychology, 1980, 32: 3-25
- [2] 章毓晋. 图像理解与计算机视觉[M]. 北京: 清华大学出版社, 2000: 248-250
- [3] 贾允, 丁艳, 刘泽平. 改进图像阈值分割算法的研究[J]. 光学技术, 2005, (1): 155-157
- [4] Jo Yew Tham, Shen Luan Lee, et al. A general approach for analysis and application of discrete multi-wavelet transforms[J]. IEEE Trans on Signal Processing, 2000, 48 (2): 457-464.
- [5] 过润秋, 张颖, 林晓春. 基于形态滤波的红外小目标检测方法[J]. 激光与红外, 2005, (6): 451-453
- [6] 夏庆观, 陈桂, 盛党红. 基于小波变换的多源图像数据融合与边缘检测方法[J]. 微计算机信息, 2005, 10-3: 105-106

## 作者联系方式

通信地址: 重庆通信学院通信指挥系

邮政编码: 400035

联系电话: 13228689768 023-68759640

# 协同通信在无线网络融合中的应用方案

潘成康 蔡跃明 徐友云 姜青竹

**摘 要：**无线接入技术是军用无线移动应用的基石之一。随着网络融合特别是以多媒体为汇聚点的业务融合的步伐加快，对业务的时延、带宽和移动性要求越来越高。因此，无线网络结构的革新和共性关键技术性能的增强成为一项紧迫任务。在探讨协同通信基本原理基础上，给出了协同通信在网络结构演进和增强通用关键技术方面的应用方案。

**关键词：**军事移动应用；网络架构；协同通信

## 1 引言

军用无线通信系统是军事信息系统重要的组成部分。为适应日趋复杂的战场环境和满足新的军事应用需求，军用无线通信系统网络化和融合集成已成必然趋势。网络融合在业务融合、核心网融合、接入网融合、终端融合等多方面可为军事移动应用提供强大动力，而业务、控制、承载和接入分离的统一构架（图 1 所示）为军事业务的灵活配置和生成奠定了基础<sup>[1]</sup>。纵观扩频通信技术、超宽带技术、Bluetooth、无线射频识别技术、Ad-Hoc、无线传感器网以及认知无线电技术的发展历程，可以清晰看到人们在军用无线接入技术方面所做出的巨大努力和成就。融合的军用无线通信系统有望带来更丰富、更可靠和更安全的军事移动业务并实现移动泛在战场环境（MUCE）。

业务层	Parlay/OSA
控制层	IMS/软交换
承载层	IP/MPLS
接入层	各种无线接入方式

图 1 分层网络架构

应该看到，在分层架构中虽然移动业务与底层网络及终端类型无关，但业务开发与应用仍然与网络和终端的能力息息相关。目前，移动多媒体业务应用的最大瓶颈是数据传输带宽、移动性、延时性能以及安全性。为突破这些限制因素，人们发展、探讨了很多全新的无线通信技术。从关键共性技术层面看，诸如 OFDM/MIMO/ARQ/HARQ/先进信号处理/网络信号处理/信源-信道编解码技术/扁平化网

络结构和 mesh 拓扑结构等技术得到一致认可。

应当意识到，任何新技术都有其性能局限性或制约其性能发挥的因素存在。为此，探索普适的增强型技术来弥补现有技术的不足成为人们的努力目标。这其中，协同通信技术以其广泛的适用性和潜在性能优势得到高度重视。

## 2 协同通信原理

协同通信<sup>[2]</sup>（cooperative communication）是利用信号的广播特性，通过中继转发信号并在接收端联合处理源信号和协同中继信号从而提高传输质量和效率的一种无线通信技术。简单说，它是多跳通信与直接通信并行融合的方案。协同通信的中继节点（R）既可以是具有转发功能的移动节点（MS），也可以是专用的中继站，既可以是一个，也可以是多个。基本的协同通信模式如图 2（a）所示，首先源节点广播信息至中继节点和目的节点，如接入点。然后中继节点转发接收的信息至目的节点。目的节点通过合并两次接收到的信号联合解调源节点信息。图 2（b）为协同通信最常见的应用形式，可以具体衍生为以下几类传输模型：① 协同多址接入，该模型支持源节点同时接入。② 协同广播，该模型支持单播和广播业务。③ 协同接收，该模型特别适合点对点传输，例如在无线传感器网络中。④ 协同发送，该模型适用于中继节点靠近源节点的情况。图 2（c）为基于协同通信的信息交互模式，适用于对等业务传输。

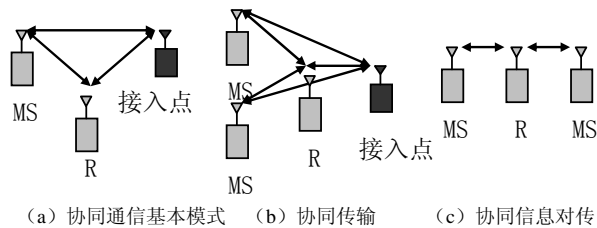


图2 协同通信模型

### 3 无线网络融合构架

#### 3.1 无线网络结构基础

传统无线网络（拓扑）结构有三类，如图3所示。图3（a）为点对多点（PMP）结构，或称集中控制结构。图3（b）为多点对多点结构，或称自

组结构。图3（c）为混合结构（集中+自组）。PMP为单跳系统，结构简单，无需路由和节点位置信息，可扩展性好，但需要基础架设的支持，网络战时的抗毁性和顽存性较差。自组结构，即网状拓扑结构，或称多跳结构或对等结构，常用于Ad-Hoc网和WSN等自组网中。自组结构中，节点地位平等可实现对等通信，而且每个节点都有多条路径到达目的节点。因此，自组结构具有支持移动节点随机部署和快速组网的能力，以及容故障能力强、组网灵活和覆盖性好的优点。但同样存在路由维护和修复困难、可扩展性差的缺点。混合网力求兼具PMP网的简洁以及网状网覆盖性好等优点，是集中式网络结构和分布式网络结构的折衷方案。但随着业务规模的增大和对QoS要求的提高，网络结构仍需演进。

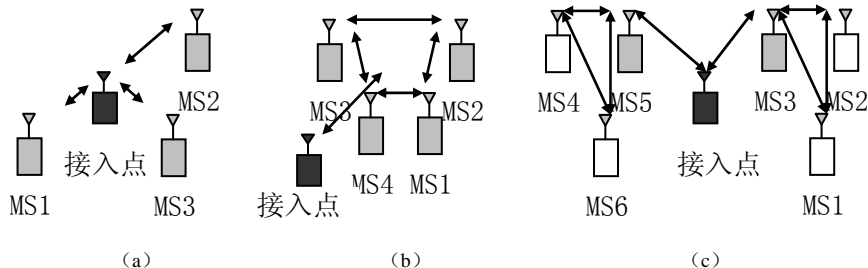


图3 无线网络基本结构

#### 3.2 无线协同中继网结构

我们可以从如何改进PMP结构和网状网结构角度来寻求网络结构演进路线。改进PMP可以布置多个接入点，使接入模块尽量靠近移动节点，或者如图4（a）所示，将天线与接入点分离，用有线连接，可以任意延伸。但是该类网络结构在回程成本和信号处理时延上存在不足。改进网状网结构可以采用无线mesh网结构<sup>[3]</sup>，如图4（b）所示。无线mesh网的提出主要也是为了扩展集中式控制网

络的覆盖范围。与Ad-Hoc网络一样，网络中的每个节点都具备路由的功能，每个节点只和邻近节点进行通信。相比于单纯的Ad-Hoc网结构，无线mesh网具有较好的可扩展性以及和蜂窝网/WLAN的兼容性。而相比于PMP结构，无线mesh则具有诸如节能、自配置、自愈性和易扩容等诸多优势。当然，构建一个高性能的无线mesh网络将面临着诸如兼容性、共存性、安全性、QoS保证等多方面的挑战。

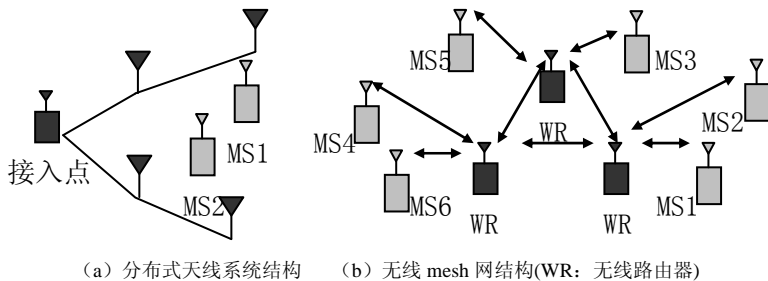


图4 无线网络演进结构

无线 mesh 技术用于宽带网络接入的相关标准是 IEEE 802.11s/n、IEEE 802.16e、IEEE 802.15.5 以及 802.20。IEEE 802.15.5 扩大了以短距离通信为手段的无线个域网 (WPAN) 的覆盖范围以及吞吐量,特别是 UWB 系统,可实现单兵战场的末端连接。无线 mesh 网中的节点分为两类:从节点和主节点。主节点构成主 mesh 网,而从节点没有到接入点的直达路径。主节点可设置为专用无线路由器 (WR), 各类从节点以 WiFi 方式接入主节点。而且,主节点并不只属于一个接入点,可以同时与多个接入点通信,而接入点之间亦可相互通信,对主节点信号进行分布式协同处理。

移动节点转发功能的增强,使得中继传输已成为网络结构革新的基本手段。既然协同通信是以中继为基础的通信技术,必然可以应用到无线 mesh 网中。基于此,我们给出一种新网络模型:无线协同中继网 (Cooperative relaying networks, COREN), 如图 5 所示。COREN 与无线 mesh 网结构类似,最大的区别在于信号处理方式。以 MS7 与接入点 MR 通信为例,有两条合适的多跳路径:MS7→MS2→MR 和 MS7→MS1→MR。如不采用协同通信,则会选择一条路径接入,例如前一条,BS 只处理 MS2 转发的信号。而采用协同通信,BS 则会联合处理 MS7 的信号和 MS2 的信号。另外,MS2 和 MS1 可以同时接收 MS7 的信号,于是 MS2 和 MS1 也可以同时转发 MS7 的信号到 MR。显然,后两种协同通信方式性能要优于非协同通信方式。COREN 中的其他典型的信号处理问题将在第 4 节中继续分析。

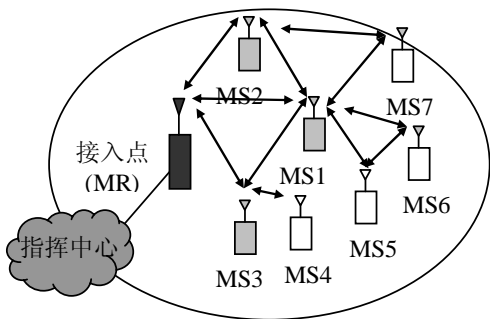


图 5 无线协同中继网参考模型

4 协同通信其他应用方案

4.1 协同MAC协议

如上所说,业务时延和传输质量是移动业务应

用的关键。接入时延很大程度上取决于链路竞争排队重传时延,而传输质量则受到各类干扰的制约,这在 Ad-Hoc 网和 WSN 中更为明显。

这里并不考虑具体的协同 MAC 算法结构和帧结构,我们只重点阐述协同通信改善媒体接入控制协议性能的思路。在协同 MAC 方案中,如图 6 所示,需要在适当位置安置一个或数个中继站 (更实际的措施是指定几个合适的 MS 担任中继节点)。当若干个源节点同时向接入点发送信息时,指示中继节点与接收端一样接收信息,然后在后续指定时隙或频段内转发接收到的信号。接收端利用多次接收的信号采用一定的合并准则解调所有源节点信号。可以看出,协同 MAC 协议在一定条件下可同时获得时间分集增益和空间分集增益,同时由于用户无需等待和回避,因此具有较高的接入效率。传统 MAC 协议性能会随着 MS 数量的增加而下降,不具备可伸缩性 (scalability)。而协同 MAC 协议随着 MS 数量的增加性能反而有所提升。当然协同 MAC 协议的性能建立在严格的帧结构设计、充足的缓存容量和较复杂的信号处理之上,在实际应用中还有待完善。

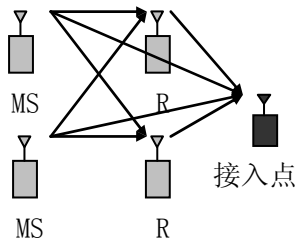


图 6 协同多接入策略

4.2 协同ARQ/HARQ

ARQ/HARQ 是移动业务 QoS 保证机制中重要的一环,实质是数据包检测错误后的一种重传机制。传统的 ARQ/HARQ 技术都只是要求 MS 自身重传数据,如果 MS 的信道具有很强的时间相关性 (MS 处于静止、徒步状态),则需要更多的重传次数。解决这一问题一个有效的办法就是采用协同 ARQ/HARQ 机制。与传统 ARQ/HARQ 不同的是,协同 ARQ/HARQ 需要设置一个适当的中继节点 (固定中继或指定其他 MS),在接收端对源节点数据包检测错误的情况下,由中继节点重传数据包。由于源节点和中继节点位置独立性,重传数据包之间可以保持低相关性,因此获得更高的码合并增益。当然,这里要求中继节点能够正确译码,如

果不存在这样的中继节点,则由 MS 自身重发。此外,应用协同 ARQ/HARQ 还需要考虑中继节点处理能力、以及额外的信令负荷等因素。

### 4.3 协同单播路由

通常研究的路由协议即指单播路由协议,分为单径路由图 7 (a) 和多径路由 7 (b) 两种。单径路由在 Ad-Hoc 网和 WSN 中研究已很成熟。路由协议影响移动业务的 QoS 主要体现在传输时延和中断率。在复杂的无线环境中,中断似乎不可避免。为此把单径路由扩展到多径路由并在多径路由上均衡能耗是有价值的思路。多径路由可以提供备份路径以防主路径失效。多径路由有两种:不相交路径以及缠绕路径(即容许冗余路径与主路径相连)。显然,维持多径路由会增加协议开销和复杂度以及网络成本。为改善单径路由协议同时避免多径路由的缺点,可以采用协同路由策略,如图 7 (c) 和 7 (d) 所示。I 型协同路由在单径路由上改进,不需要额外的备选路径,只需要额外的信号合并处理。在传统单径路由中,每个节点只接收前一跳的信号,对此之前的信号不予理睬。而 I 型协同路由容许下游所有节点接收前跳的信号,这些存入缓存的信号逐级合并直至能够正确解调。很显然, I 型协同路由可以有效降低单径路由的中断概率,同时可以减少路径中的传输跳数,进而降低传输时延。如果在 I 型协同路由基础上,适当增加中继路由节点(路由节点数远少于多径路由中的冗余节点数),可以得到 II 型协同路由。II 型协同路由结构上有些类似缠绕多径路由,但两者有本质不同:前者增加中继节点是为了提供冗余信号,而后者增加路由节点是为了提供冗余路径(当然 II 型也可以提供冗余路径)。

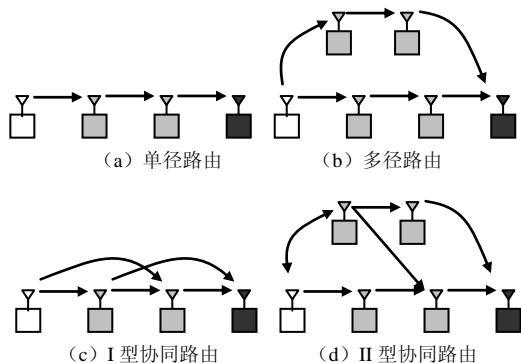


图 7 不同类型的路由方案

### 4.4 协同切换

切换是移动应用最直接的支撑技术。802.21 基于移动 IP 协议在异构接入网层面上制定了统一的切换和漫游标准。然而,该标准没有具体的机制保证无缝切换(即低时延、低丢包率),因此需要进一步改进。影响切换性能有两个因素:阻塞率和传输质量。传统切换决策通常会在接收信号强度和小区阻塞率两个参数间为难,利用协同切换可以更好的解决这个问题。协同切换的思路简单的说就是利用协同通信技术进行负载均衡,其唯一准则是接入到业务负荷最轻的临近小区,利用协同多跳的方案(参见 I 型协同路由)确保接入传输的可靠性。协同切换中,移动端首先发起切换接入请求,业务负荷最轻的接入端根据网络连通状态计算路由信息并为移动端指定接入路径(即指定中继为移动端提供路由),同时分配相应带宽。协同切换在高速移动通信环境和大密度业务环境中有很好的应用。

### 4.5 其他应用场景

对于数字战场无线接入承载环境,协同通信可以有效支持同构或异构终端之间的通信,为宽带业务提供 QoS 保证。协同通信可以充分挖掘 MIMO 技术潜力,扩展 MIMO 技术的军事应用范围。认知无线电在军事领域已得到关注,协同频谱感知技术有望为无线通信抗干扰带来新途径。

## 5 网络融合对终端功能需求

军事移动业务应用(如多媒体信息业务、流媒体业务和定位业务等)越来越依赖于终端的支持。在异构化的融合网络中,终端处理能力的强弱,直接决定了业务丰富程度、体验品质和安全性。在网络分层架构中,终端业务平台与网络应用平台已处于平等地位。新的业务和新的通信技术对终端功能需求包括:

- 多模功能,支持异构网间的切换。
- 音视频编解码器、简便的操作系统和界面,大的存储空间。
- 路由转发功能,用于多跳网、mesh 网和协同通信。

目前随着大批厂商的加入,移动终端的处理芯片、处理能力、存储能力均飞速提高,伴随良好的

操作系统的开发与支持，智能终端发展已成主流趋势。

## 6 结束语

军事移动业务的快速发展，对底层无线接入网络的业务能力提出了越来越高的要求，革新无线网

络结构和增强无线通信关键技术性能势在必行。协同通信充分利用网络中的信号冗余并通过信号合并处理有力地提高了无线链路的传输质量，这种优势将在网络结构革新和关键技术改进上得到充分利用。

### 参考文献

[1] 卢美莲，程时端. 网络融合的趋势分析和展望[J]. 中兴通讯技术，2007，13（1）：10-13.

[2] HUNTER T. E., HEDAYAT A. Cooperative Communication in Wireless Networks [J]. IEEE Communication Magazine, 2004, 42（10）：74-80.

[3] AKYILDIZ I. F., WANG X., WANG W. Wireless Mesh Networks: A Survey [J]. Computer Networks, 2005, 47（1）：445-487.

### 作者联系方式

通信地址：江苏南京御道街标营 2 号通信工程学院  
邮政编码：210007  
联系电话：025-80828394      13813899983

# 基于BP神经网络的C<sup>4</sup>ISR通信系统效能评估

屈洋 秦伟 苏鹏

**摘 要:** 为评估 C<sup>4</sup>ISR 通信系统效能,最大程度地提高 C<sup>4</sup>ISR 系统整体效能,采用神经网络评估 C<sup>4</sup>ISR 通信系统效能,按照建立 BP 网络模型、设计模型结构及确定训练样本的步骤,实现神经网络评估模型创建的全过程。该模型把各个评估指标作为输入,通过历史数据的训练确定神经网络输入、输出的对应关系,从而得出系统的效能值。神经网络评估模型可动态地评估 C<sup>4</sup>ISR 通信系统的效能,其评估过程确定的各指标项相互关系与系统的效能有密切的关系,正确地对它们进行评估对于研究 C<sup>4</sup>ISR 通信系统的效能具有重要意义。

**关键词:** BP 神经网络; C<sup>4</sup>ISR 通信系统; 效能评估

## 1 引言

随着大量高技术武器装备在战争中的使用, C<sup>4</sup>ISR 系统在战争中的作用越来越重要,被称之为兵力倍增器。C<sup>4</sup>ISR 通信系统作为 C<sup>4</sup>ISR 系统的一个重要的子系统,它的效能对整个 C<sup>4</sup>ISR 系统效能的影响至关重要,因此研究 C<sup>4</sup>ISR 通信系统的效能评估为更好地研究 C<sup>4</sup>ISR 系统奠定了基础。

目前,系统效能评估的方法有很多种,而神经网络模型具有很强的非线性映射能力和柔性网络结构,以及高度的容错性和鲁棒性,评估过程中可以减少许多人为因素的影响,因此,本文尝试采用 BP 神经网络的方法,对 C<sup>4</sup>ISR 通信系统的效能进行评估,为 C<sup>4</sup>ISR 系统性能的改进和效能的提高提供理论依据。

## 2 C<sup>4</sup>ISR通信系统效能评估指标体系的建立

C<sup>4</sup>ISR 通信分系统效能评估涉及系统全生命周期,所以必须建立科学合理的指标体系才能对系统进行评估,得出合理的结论。通过对 C<sup>4</sup>ISR 通信分系统的分析,其通信分系统效能评估的指标体系可以分成三层,包括网络可靠性(广义)、抗毁生存能力和战时通信能力,每层指标又有不同的子指标,如图 1 所示。

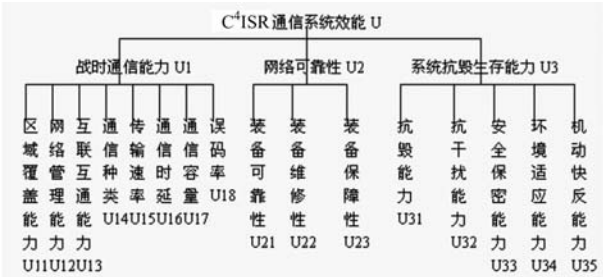


图 1 C<sup>4</sup>ISR 通信系统评估指标体系

## 3 基于BP算法的C<sup>4</sup>ISR通信系统效能评估模型

系统分析的目的是为了根据问题的特征优选出适合于解决所遇应用问题的某种网络模型。对于映射分类问题,比较适合的网络是非线性前馈网络,本文采用 BP 网络模型,其结构如图 2 所示。BP 神经网络的输入与输出关系是一个高度非线性映射关系,如果输入节点数为  $n$ ,输出节点数为  $m$ ,则网络是从  $n$  维欧式空间到  $m$  维欧式空间的映射。

对于解决 C<sup>4</sup>ISR 通信系统效能评估这一类复杂的非线性问题, BP 神经网络有其独特的优势,本文采用三层 BP 神经网络对 C<sup>4</sup>ISR 通信系统效能进行评估,神经网络输入层节点为 16 个,分别对应评估指标体系最底层的 16 个指标,隐层节点数初始定为 10(在训练过程中可视网络的泛化能力调整),输出节点数为 5,分别对应于优、良、中、差,很差 5 个效能评估等级。神经元输入与输出之间转移函数选取 Sigmoid 函数:

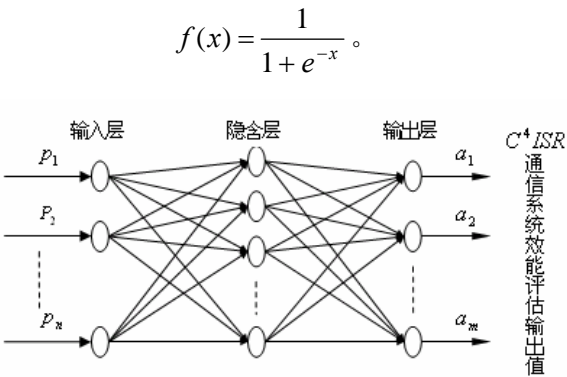


图2 三层  $C^4ISR$  通信系统 BP 神经网络评估模型

3.1 BP算法的流程

若 BP 神经网络分为三层，第一层为输入节点层，第三层为输出节点层，则 BP 学习算法描述如下。

1) 权值和神经元阈值初始化。给所有权值和阈值赋以在[0, 1]上分布的随机数。

2) 输入样本模式，指定输出层各神经元的期望输出值  $a_1, a_2, \dots, a_m$ 。

$$a_j = \begin{cases} 1 & p \text{ 属于第 } j \text{ 类} \\ 0 & p \text{ 不属于第 } j \text{ 类} \end{cases} \quad j = 1, 2, \dots, m$$

3) 依次计算每层神经元的实际输出，直到计算出输出层各神经元的实际输出  $(a_1, a_2, \dots, a_n)$ 。

4) 修正权重。Back-Propagation 三层神经网络的权重按照下列方法修正：网络的权重按随机方式初始化（例如随机取[-1, 1]之间的数依次赋值），然后根据每个样本值与网络输出的误差，轮番逐个修改网络的权重，直至达到某个规定的条件。BP 网络按梯度法修改权重并反向传播，即从输出层开始，逐步向后递推，直到第一隐含层。

5) 转到（2）。如此循环，直到全部误差满足给定条件为止。

BP 学习算法流程如图 3 所示。

3.2 样本的归一化处理

样本的原始数据必须经过归一化处理，才能用来真正训练神经网络，在这里将采用线性变换的方法将原始样本转变为训练样本。此方法分为两种情况。

1) 当指标越大效能越好时，按公式①进行归一化。

$$Y = \frac{X - \min}{\max - \min} \tag{1}$$

2) 当指标越小效能越好时，按公式②进行归一化。

$$Y = \frac{\max - X}{\max - \min} \tag{2}$$

式中，X 为原始训练样本值，Max（或 Min）对同一指标而言可能出现的最大值（或最小值）。

3.3 BP算法训练神经网络及具体应用

用来训练神经网络的样本的选取很重要，它直接关系到评估结果的可信度问题。为了使评估的结果符合实际，以真正反应  $C^4ISR$  通信系统效能，本文通过以下方法获得原始训练样本。

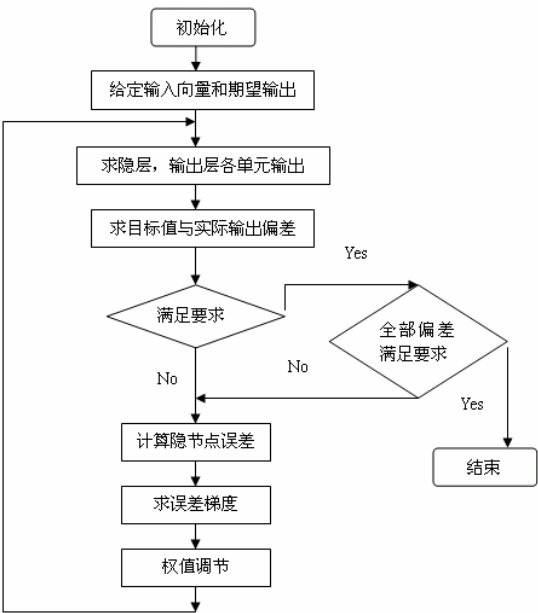


图3 BP 学习算法流程图

以  $C^4ISR$  通信系统相对应的各指标数据为神经网络输入值，并通过专家打分的方法，给出该  $C^4ISR$  通信系统效能评定值，将其作为输出值。表 1 列出了经过归一化处理后的样本值，其中，输入值为系统对应的 16 指标的评估值，可以认为若评估值都在 0.9 以上，则系统效能为优，在 0.8~0.9 之间为良，在 0.6~0.8 之间为中等，在 0.5~0.6 之间为差，0.5 以下为很差。N1~N5 对应优，良，中，差，很差五个评估等级。



表 1 训练样本值

样本		输入值															输出值					
		U11	U12	U13	U14	U15	U16	U17	U18	U21	U22	U23	U31	U32	U33	U34	U35	N1	N2	N3	N4	N5
训练样本	1	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	1	0	0	0	0	
	2	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0	1	0	0	0	
	3	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0	0	1	0	0	
	4	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0.55	0	0	0	1	0	
	5	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0	0	0	0	1	
	6	0.95	0.95	0.75	0.85	0.15	0.45	0.42	0.25	0.46	0.28	0.12	0.15	0.35	0.52	0.42	0.35	1	0	0	0	0
	7	0.85	0.85	0.42	0.12	0.55	0.65	0.24	0.34	0.56	0.45	0.25	0.34	0.36	0.28	0.29	0.37	0	1	0	0	0
	8	0.70	0.70	0.18	0.25	0.45	0.13	0.28	0.24	0.16	0.19	0.27	0.26	0.19	0.26	0.34	0.28	0	0	1	0	0
	9	0.55	0.55	0.32	0.12	0.25	0.16	0.34	0.12	0.18	0.19	0.25	0.27	0.23	0.13	0.17	0.24	0	0	0	1	0
	10	0.45	0.45	0.13	0.09	0.08	0.14	0.18	0.13	0.16	0.08	0.12	0.25	0.26	0.34	0.28	0.19	0	0	0	0	1
验证样本	1	0.85	0.85	0.86	0.12	0.36	0.45	0.26	0.34	0.18	0.27	0.34	0.29	0.16	0.27	0.35	0.26	1	0	0	0	0
	2	0.85	0.23	0.34	0.38	0.29	0.54	0.26	0.34	0.16	0.19	0.34	0.26	0.54	0.58	0.68	0.38	0	1	0	0	0
	3	0.45	0.25	0.36	0.24	0.16	0.08	0.34	0.29	0.36	0.45	0.16	0.27	0.48	0.26	0.35	0.46	0	0	0	0	1

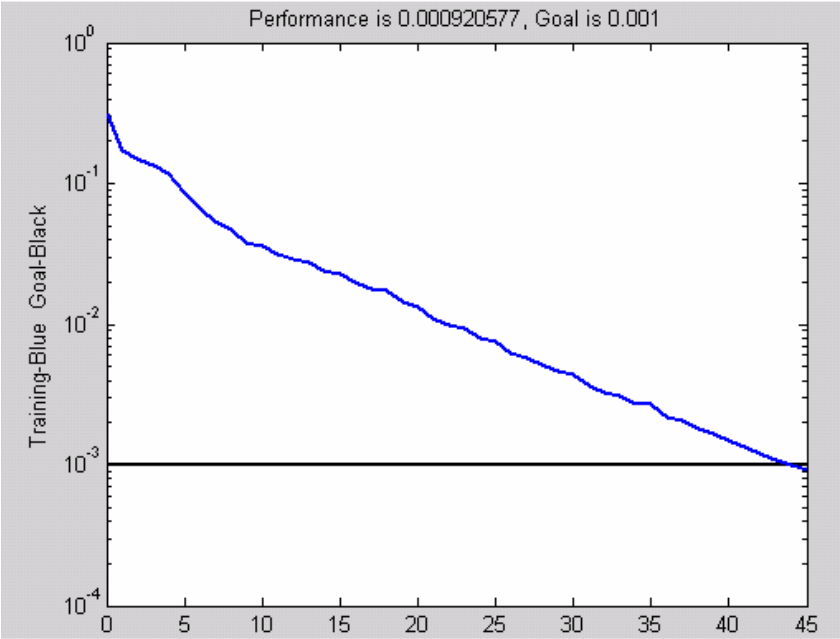


图 4 BP 神经网络效能评估仿真图

根据前面的分析，利用 Matlab 编写神经网络应用程序，将归一化后的十个样本用于神经网络的训练。并将 3 个验证样本进行检验，经过反复地学习，第一组样本评估值为：[0.019109, 0.97353, 0.00018088, 0.27696, 0.000018565]，显然，系统

效能为“优”级；第二组样本评估值为：[0.0030287, 0.99762, 0.21208, 0.0000447, 0.0000163]，效能为“良”级；第三组样本评估值为：[0.0003622, 0.0000018, 0.00056041, 0.0005029, 0.99666]，效能为“很差”级，满足精

度要求 ( $E < 0.001$ ), 训练如图 4。

经检验该神经网络的输出值与专家评估值是一致的, 已具备了模式识别的能力, 可用于评估  $C^4ISR$  通信系统的作战效能。以某  $C^4ISR$  通信系统为例, 若其 16 项指标的评估值分别为 [0.85, 0.83, 0.84, 0.88, 0.75, 0.79, 0.82, 0.78, 0.81, 0.86, 0.74, 0.86, 0.75, 0.82, 0.73, 0.85], 则神经网络的输出值为: [0.12604, 0.53016, 0.0064089, 0.0000832, 0.00090684], 显然, 可以判断该  $C^4ISR$  通信系统效能为良。

## 4 结束语

本文建立了  $C^4ISR$  通信系统综合评价指标体

系, 并应用 BP 神经网络进行了  $C^4ISR$  通信系统的综合评价, 实验表明, 该方法运算速度较快, 可靠度较高, 能够进行定量分析, 得出了  $C^4ISR$  通信系统的评估结果, 实现了计算机作为“评价专家”来代替人进行评价, 并取得了很好的效果, 为提高  $C^4ISR$  系统的整体效能提供了有价值的参考。

但采用该方法也有一些不足之处, 主要表现在以下几个方面: ① 中间层数目、各层神经元个数、学习因子和循环次数等都需要根据问题结构由算法设计者依照个人经验确定, 存在一定的主观性; ② 神经网络方法很多时候只是局部最优, 在某些情况下会出现过拟合现象。

## 参考文献

- [1] 柏晓莉等.  $C^4ISR$  系统通信网络效能评估指标体系研究[J]. 军事运筹与系统工程, 2006, (1): 71-75.
- [2] 赵策等. 基于灰色关联分析的  $C^4ISR$  通信系统效能评估[J]. 武器装备自动化, 2007, (2): 3-5.
- [3] 顾吉堂等. 应用神经网络评估舰载武器系统作战效能[J]. 指挥控制与仿真, 2007, (2): 66-70.
- [4] 郝海燕等. 精确制导武器系统作战效能的 LMBP 神经网络评估[J]. 情报指挥控制系统与仿真技术, 2005, (6): 26-29.
- [5] 祝金荣等. 基于 BP 神经网络的信息对抗能力综合评价研究[J]. 情报技术, 2006, (2): 5-6, 11.

## 作者联系方式

通信地址: 安徽蚌埠坦克学院研究生队

邮政编码: 233050

联系电话: 13695525695

# 面向高可用网络的ospf平稳重启技术研究

商云飞 詹武

**摘 要：**高可用性的网络是军队信息化发展的基础和必然需求。实现网络的高可用性技术作为军队信息化的关键技术，值得我们深入地研究和发。本文针对高可用性网络的需求，提出了高可用网络的一些关键技术，深入分析了面向高可用网络的 ospf 平稳重启技术，并详细阐述了平稳重启实现时所采用的关键技术。

**关键词：**ospf 路由协议；高可用网络；平稳重启；无中断转发

## 1 引言

现代化的战争是高科技的战争、信息化的战争，军事信息系统能否高效、可靠、稳定的交互信息在整个战争中占有着举足轻重的地位。所以军事信息系统的网络高可用技术成为了军队信息化建设的一个关键技术，对作战信息的稳定、可靠传输乃至整个战争的成败具有重要的意义。

本文对支持高可用网络的 ospf 路由协议<sup>[1]</sup>的平稳重启技术进行了深入研究，首先介绍了高可用网络的关键技术；随后深入分析了平稳重启的原理、重启阶段的过程细节以及平稳重启意义；最后分析和讨论了实现基于 OSPF 协议的平稳重启的关键技术。

## 2 高可用网络的关键技术

### 2.1 高可用网络技术概述

根据系统可靠度的不同，可以将系统分为四个档次：连续可用性系统（Continuous Availability System）、容错系统（Fault Tolerance System）、高可用系统（High Availability System）、容灾系统（Disaster Tolerance System）<sup>[2]</sup>。对于军事信息系统网络中的路由器等网络设备，要求至少达到高可用系统的要求。

网络可用性是指网络节点之间在能够保证质量要求的前提下传输数据的时间占总时间的百分比，是衡量网络质量的重要指标之一。决定网络可用性的关键技术包括路由快速收敛技术、快速重路由（FRR）<sup>[3]</sup>技术、软硬件在线升级技术、协议平稳

重启技术、设备自身可靠性技术。

提高可用性的途径有很多，归纳起来有以下几个途径：提高系统组成部件的冗余度，用成本换取可靠性；高可用和高可维的体系结构设计，在网络结构设计方面提高可用性；将复杂系统进行模块化切分，用提高工作量换取可用性；使用规范的工程设计和工程管理方法，提高可靠性和可维性。

评估和建设一个高可用性的网络是一个庞大的系统工程，需要对设备可靠性、网络介质的可靠性、网络拓扑结构、设备运行环境、管理和服务等多方面进行综合分析和改进。一般在确定网络模型之后，影响整个网络可用性的几个主要因素如图 1 所示。

### 2.2 高可用网络单元

路由器和传输链路的可用性是 IP 网络可用性的基础。路由器的可用性不是靠简单地增加备用板就能解决的，而是一种设计原则，从一开始就需要纳入产品的体系架构中。硬件可靠性的主要改进措施包括从单平面交换向多平面交换演变；关键部件采取冗余设计；控制平面与数据转发平面分离等。软件可靠性的主要改进措施包括采用轻型 kernel 核心软件；软件功能模块化设计，使每个软件模块在不同的运行空间中运行不同的协议，改进软件系统的稳定性和可用性；进程最佳化以实现快速故障恢复；数据最佳化以减少子系统间必须传送的数据量，改进系统整体性能等。高可用路由器的设计原则就是采用关键系统部件的冗余设计和高效的故障管理。这里包含软件和硬件两个层次的概念，硬件的冗余结构作为软件进行故障管理的支撑平台和对象。

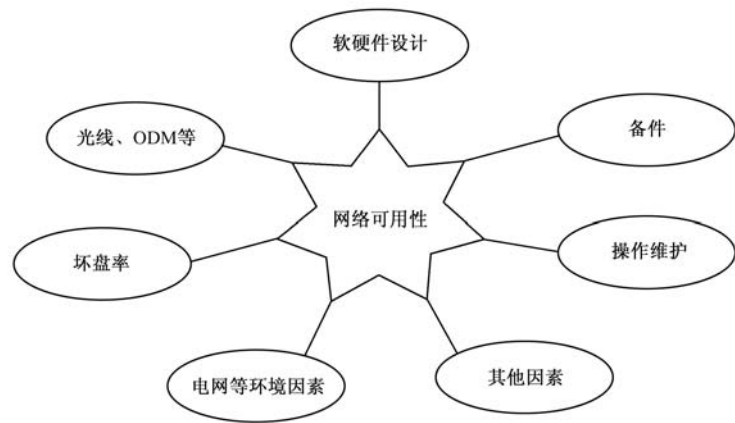


图 1 影响网络可用性的主要因素

要达到整个路由器系统乃至整个网络系统高可用的性能指标，网络设备系统软件可靠性的设计还是一个难点，它不只要解决软件本身设计中存在的缺陷，同时还要根据网络协议的特点进行相应的处理。上述关键技术是支持高可用网络的关键技术，但它们都只适用于单台路由器。要支持整个网络的高可用性，就需要对上层软件进行高可用设计。以高可用的硬件平台为基础，软件的设计应能够快速检测到软硬件故障并尽快恢复，尽可能的避免系统恢复过程中的会话阻塞。通过设置路由协议的定时器，在保留路由、转发表和会话的前提下，实现系统的快速平稳恢复，有助于消除对网络服务和应用的显著影响。IETF 对路由协议进行了扩展，提出了 OSPF 平稳重启技术<sup>[4]</sup>，使得高冗余的硬件平台与快速无缝的软件恢复技术相结合，从而提高了网络的可用性。

2.3 网络层可靠性技术

目前新出现的网络层可靠性技术主要有 IP 路由快速收敛技术<sup>[5]</sup>、LSP 保护切换、路由协议的平稳重启技术等。

(1) IP 路由快速收敛

在传统路由协议的基础上，对 IP 动态路由进行改进可以缩短 IP 路由协议的故障响应时间，这些措施主要是加快路由协议的收敛。加快路由协议收敛速度可以从链路故障检测、路由重计算、路由信息更新等几个方面考虑。通过加快链路之间 Hello 消息的发送频率，加快 SPF 计算速度和为路由更新消息设定高优先级，路由协议可以快速发现、处理故障，并且准确快速地进行路由更新，加快路由协议的收敛。另一种加快路由协议收敛的方

法是采用 IGP 和 EGP 对网络进行合理的层次规划，IGP 进行域内设备的路由，EGP 承载外部路由，两种路由之间进行有效隔离。IGP 和 BGP 的合理分工，形成了一个层次化的路由结构，域内和域间路由协议的收敛相互独立，互不影响，可以实现最快速度收敛。

(2) LSP 保护切换

为了满足诸如像视频电视电话会议这一类业务的实时应用，必须对这些流量提供 LSP 保护能力。保护切换是 ITU-T 采用的术语，保护切换技术对于提高 MPLS 网络的可用性和稳定性具有关键意义。保护切换一般对受保护 LSP 路由的预计算和资源的预分配，所以可以保证在 LSP 连接失效或者中断后可以快速重新获得网络资源。

(3) 路由协议的平稳重启 (graceful restart)

IETF 提出了针对 ISIS、OSPF、BGP、LDP、RSVP 等协议的平稳重启协议。平稳重启就是在路由器控制平面故障重启、软件升级、主备切换等情况下，数据转发平面正常工作，尽量不影响业务的正常提供。平稳重启技术是在网络稳定也就是拓扑没有变化的情况下，尽量保证业务提供。如果在协议重启期间网络拓扑发生变化，由于控制引擎不能及时进行路由计算和更新，可能造成网络路由不同步，产生路由循环或转发黑洞。协议平稳重启与快速路由收敛从不同的出发点减少业务的中断，但是存在一定的矛盾，所以在实际网络设计中要谨慎使用。

3 ospf平稳重启技术研究

在通常的网络环境中，当路由器或个别路由协

议因为某种原因重启时，路由器将失去与其邻居之间的路由邻接关系。邻居路由器在检测到邻接关系失效后，将重新计算新的路由，并向其他邻居发送路由更新报文，通告失效的邻接关系，这种更新行为将在整个网络中传递。在此期间，由于邻居路由器撤销了重启路由器先前通告的路由，重启路由器将不会从其他路由器接收到任何报文。一旦完成重启动，重启路由器将重新建立其邻接关系，邻居路由器必须再次计算新的路由，并发送相应的路由更新报文。由此导致路由抖动，生成大量的路由更新报文，给整个网络中的路由器控制平面带来较大压力。如果网络中同时存在大量的路由更新报文或同时有多个路由器重启，那么网络中所有的路由器都将受到影响。

在网络中引入平稳重启技术可以将上述缺陷造成的负面影响最小化。平稳重启技术是支持高可用网络协议级的重要技术，其目的是在不引起网络中路由抖动的前提下实现路由器的平稳重启，使路由协议重启的影响最小化。路由抖动会引起网络资源的浪费，其中包括路由计算资源的浪费和网络带宽的浪费。平稳重启允许路由器在短时间重启期间仍然转发报文，而其邻居路由器将向网络中其他路由器屏蔽重启事实，同时也将继续向重启路由器转发报文。这样，就将网络重新汇聚的代价减到最小，同时又保证了无中断转发。若路由器在一段时间内仍未启动（可以通过计时器来设定时间门限），则认为该路由器处于 down 状态，此时为了保证路由转发的正确性，不采用平稳重启技术。在成功进行平稳重启之后，路由器只需付出极小的代价重新进行拓扑计算，丢弃极少的报文就可以重新加入网络。平稳重启与无中断转发相结合，在无中断转发所提供的转发平台稳定性之外进一步增强了整个网络级控制平面的稳定性。

平稳重启的整个过程是从路由器重新启动或装载算起，直到重新与先前的 FULL 邻接的邻居路由器重新建立 FULL 邻接关系为止。在平稳重启过程中，路由域中的路由器分为三个角色<sup>[6]</sup>。

- 1) 重启路由器 (RR): 要进行重启的路由器。
- 2) 协助路由器 (HR): 重启路由器的 FULL 邻居。
- 3) 其他路由器 (OR): 路由域中的其他路由器。

我们从重启路由器的角度将 OSPF 协议平稳重启分为三个阶段，即：能力协商阶段，平稳重启阶段，收尾阶段。

在重启之前，重启路由器 (RR) 通过向其所有的 FULL 邻居发送 `grace-lsa`<sup>[4]</sup> 与邻居路由器进行能力通告，如果所有 FULL 邻居都确认愿意作为 HR 协助 RR 完成平稳重启，并且 RR 收到了所有 FULL 邻居的确认，则说明协商成功，RR 可以在 HR 的协助下开始重启。

重启过程中，HR 通过继续在链路状态通告中将 RR 通告为 FULL 邻居，向路由域中的 OR 屏蔽 RR 的重启事件，这样就避免了路由域范围内的一次路由抖动。由于控制与转发分离，HR 仍然能够按照重启前的转发表继续转发数据。当 HR 完成重启准备退出平稳重启时，HR 仍然向路由域中其他路由器屏蔽 RR 的状态变化，避免第二次路由抖动，并配合 RR 平滑地返回正常工作状态。

## 4 实现平稳重启的关键技术

### (1) 控制转发分离技术

将路由器的控制功能与转发功能分离，两者由不同的处理器分别进行处理。专用的控制处理器负责根据从邻居收集的拓扑信息进行路由计算，将路由载入转发表中。转发可以集中于单个处理器也可以分布在多个线卡中进行。负责路由控制功能的部件常称为控制平面，负责转发功能的部件称为转发平面<sup>[7]</sup>。控制与转发分离后，转发平面从由于路由控制信息泛滥导致的网络稳定问题中隔离出来，路由器的转发行为将不会受到路由软件稳定性的影响，由于网络中的不稳定性往往导致产生大量过载的路由控制信息，而这种功能模块上的划分使得转发平面与网络中潜在的不稳定性隔绝开来，同时也减弱了路由协议崩溃可能带来的影响，使无中断转发 (non-stop forwarding) 成为可能。

### (2) 可靠能力通告技术

OSPF 平稳重启的重启准备阶段，重启路由器首先要向其所有邻居发送 `grace-lsa` 进行能力通告。如果重启路由器及其邻居都满足进行平稳重启的各项条件，只是由于网络拥塞等原因导致 `grace-lsa` 丢失或者从邻居路由器发回的 LSA 响应丢失，平稳重启将无法进行。因此，有必要保证 `grace-lsa` 的可靠传输。为了保证 `grace-lsa` 能够可靠地传送给邻居

路由器,我们令 `grace-lsa` 以 `hello` 报文的发送间隔(默认配置是 10 秒)发送 3 次,在从邻居路由器收到 `lsa` 响应之后才认为邻居路由器同意协助进行平稳重启。由于 `grace-lsa` 只是本地链路范围内的 `lsa`,即邻居路由器接收到 `grace-lsa` 之后并不会像对待一般的 `LSA` 一样向所有接口泛洪,因此多次发送 `grace-lsa` 并不会增加多少网络流量,对网络性能影响很小。

### (3) 平稳重启后的快速恢复技术

平稳重启完成后,重启路由器通过向邻居路由器发送 `hello` 报文来重新建立邻接关系,此时的 `hello` 报文中不会像重启前一样将邻居路由器列为自己的邻居,而接收到 `hello` 报文的邻居路由器也会产生错误的判断,因此浪费了重新进行网络汇聚的时间。我们在 `hello` 报文中的 `LLS` 负载中扩展重启信号字段,这样接收到 `hello` 报文的邻居不会因为 `hello` 报文中没有将自己列为邻居而认为重启路由器没有恢复,加快了重新建立邻居关系,重新进行网络汇聚的过程。

## 5 总结与下一步工作

本文对面向高可用网络的 `ospf` 平稳重启技术进行了深入研究,在路由器支持控制与转发分离的前提下,平稳重启技术用来减少由于路由器维护等原因带来的路由器控制平面的不稳定性。在重启路由器与其邻居路由器进行能力通告和协商之后,邻居路由器通过对其他路由器屏蔽短时间重启路由器的重启事实来避免路由抖动。在平稳重启顺利进行期间,网络中的报文转发行为如同路由器没有重启一样平稳进行。

我们下一步的工作是:

1) 基于对平稳重启技术的研究,在开放路由平台上,设计并实现了一个平稳重启使能的原型系统,并对这一系统进行协议一致性测试。

2) 继续对高可用性网络进行更深一步的研究,使得实现高可用性网络的途径和手段能够配合、并行、高效地使用。

## 参考文献

- [1] J. Moy, OSPF Version 2, RFC 2328, April 1998
- [2] 徐恪,吴建平,徐明伟,高等计算机网络——体系结构、协议机制、算法设计与路由器技术,机械工业出版社,2003年9月。
- [3] Matt Kolon, Delivering High Availability Routed Networks, APRICOT 2005, Kyoto
- [4] Redback Networks Whitepaper, Graceful Restart: Supporting High Availability, July 2002
- [5] Brian Daugherty, Optimizations for Routing Protocol Stability and Convergence, <http://www.cisco.com>, 2002
- [6] J.Moy, P.Pillay-Esnault, A.Lindem. Graceful OSPF Restart. RFC 3623. November 2003
- [7] L. Yang, R. Dantu, T. Anderson, R. Gopal. Forwarding and Control Element Separation (ForCES) Framework. RFC 3746, April 2004

## 作者联系方式

通信地址:北京万寿路3号

邮政编码:100036

联系电话:010-66974138      13811006239

# 军事通信网业务流建模及其仿真实现

沈宇 徐启建 钟静 陈自卫

**摘 要：**在分析军事通信网作战仿真流程及其业务流模拟步骤的基础上，给出了基于吸引系数法建立指挥所间业务流量矩阵的算法，并对语音、数据和视频业务流及其合成性能分别建模，进一步利用 OPNET 仿真软件建立了指挥所业务流合并模型，最后给出了某军事通信网作战运用的仿真实例，实现了利用仿真法定量分析和规划军事通信网作战运用的技术途径。  
**关键词：**军事通信网；吸引系数法；业务流模拟；作战仿真

## 1 引言

从军事通信网的作战保障任务出发，围绕其保障范围内各指挥所通信业务需求，通过分析和预测，确定指挥所之间各通信业务的流量和流向，并根据各业务流的特性及其综合特性，对军事通信网的战场运用进行仿真和调整，以定量和直观的分析方法指导军事通信网组织运用的规划与优化，这已成为当前科学组织和运用军事通信网的基本方法<sup>[1]</sup>。

## 2 军事通信网作战仿真的基本步骤

目前，仿真法已成为通信网性能分析和规划设计的主流方法。利用通信网仿真专用软件对军事通信网作战仿真并进行性能分析，流程如图 1 所示。

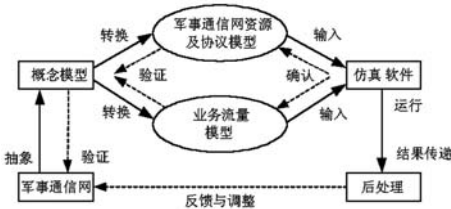


图 1 军事通信网作战仿真的流程图

首先，建立业务流量模型以描述指挥所用户对军事通信网资源的随机请求；其次，建立处理指挥所用户请求的军事通信网资源和网络协议模型；然后，对军事通信网模型进行离散事件仿真，得到模型的行为特性；最后，对模型的行为特性进行处理，主要是点估计和区间估计，获得系统性能参数。

在军事通信网作战仿真中，准确地描述业务流

的特性是对军事通信网性能进行研究、预测的前提，同时也直接关系到仿真结果的准确度和可信度，因而成为军事通信网作战仿真研究的重要内容，其一般步骤如图 2 所示。

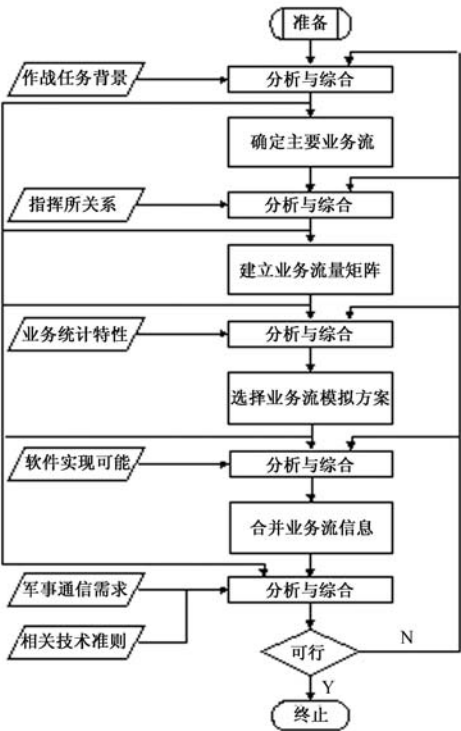


图 2 军事通信网作战仿真业务流模拟的步骤

1) 确定影响军事通信网性能的主要业务流。军事通信网的业务流具有复杂的战场特性，必须明确网络上需要和可能传输的业务流的类型，哪些是影响网络性能的主要业务流，哪些需要模拟，哪些对整个网络性能影响甚小可以不予考虑。

2) 建立军事通信网业务流量矩阵。明确了要考虑的业务类型后，还必须进一步分析各业务的流量及流向，知道主要是什么指挥所的哪些业务终端

向网络产生了流量, 如何对各业务流分类和确定各终端所在指挥所用户群在网络中的地理位置分布等。

3) 确立军事通信网业务流模拟方案。建立了业务流的类型及其流量矩阵后, 还应对业务流采用的模拟方法做出选择。对单个业务而言, 必须根据其统计特性分别进行模拟, 同时还要对同种业务的叠加特性进行综合考虑。

4) 合并军事通信网业务流信息。明确了各业务流的模拟方案后, 还要根据所选用的通信网络仿真软件提供的实现技术, 把各业务流的流模型在仿真软件中具体实现和综合, 为仿真提供离散事件输入。

### 3 军事通信网业务流量矩阵的建立

建立业务流量矩阵的方法<sup>[1]</sup>很多, 目前在民用网中, 计算局间业务流量的方法大致可归纳为两大类: 一类为比例分配方式, 包括比例分配法, 双因素变换法等; 另一类是建立数学模型, 包括引力法、吸引系数法等。其中吸引系数法在工程设计中经常使用, 它也适用于军事通信网话务流量的预测。其基本思想是: 规定两局间的话务流量与发话局的总发话话务量及受话局的总受话话务量的乘积成正比, 而与全网各局的总发话话务量成反比, 并乘以两局间的吸引系数, 计算公式如下式:

$$X_{ij} = K_{ij} \frac{O_i T_j}{\sum_{i=1}^n O_i} \quad (1)$$

式中:  $n$  为全网局数;  $O_i$  为  $i$  局的总发话话务量;  $T_j$  为  $j$  局的总受话话务量;  $K_{ij}$  为  $i$ 、 $j$  局间吸引系数, 它表示两局间用户的关切程度。

在军事通信网中, 话音业务是主要业务之一, 但其在通信业务总量中所占比例逐渐减小, 数据业务和视频业务需求急剧增加。为了对军事通信网通信业务的需求结构有更为准确和翔实的描述, 在采用吸引系数法时, 应对军事通信网保障范围内各指挥所间的话音、数据和视频业务分别进行流量预测, 按业务类型建立各自相应的业务流量矩阵, 具体运用和改进如下:

$$F_{ij} = C_{ij} \frac{D_i A_j}{\sum_{j=1}^n A_j C_{ij}} \quad (2)$$

式中:  $n$  为军事通信网内指挥所的总数;  $F_{ij}$  为第  $i$  指挥所至第  $j$  指挥所的某业务流量;  $D_i$  为第  $i$  指挥所的某业务去话话务量;  $A_j$  为第  $j$  指挥所的某业务来话话务量;  $C_{ij}$  为第  $i$  指挥所与第  $j$  指挥所间的吸引系数, 它表示指挥所间关切程度。其中:

$$D_i = N_i P R_i \quad A_j = N_j P Q_j \quad (3)$$

式中:  $N_i$ 、 $N_j$  分别为指挥所  $i$ 、 $j$  的某业务用户数;  $P$  为某业务每个用户的峰值平均业务量, 该数据可以取多个值作多方案比较;  $R_i$ 、 $Q_j$  分别为指挥所  $i$ 、 $j$  某业务的去话和来话业务量在  $i$ 、 $j$  指挥所全部该业务量中所占的比例。

根据上述吸引系数法的公式, 将公式 3 代入公式 2, 可得:

$$F_{ij} = \frac{C_{ij} N_i R_i N_j Q_j}{\sum_{j=1}^n C_{ij} N_j Q_j} \times P \quad (4)$$

如果令

$$S_{ij} = \frac{C_{ij} N_i R_i N_j Q_j}{\sum_{j=1}^n C_{ij} N_j Q_j} \quad (5)$$

则 2 式可写成

$$F_{ij} = S_{ij} \times P \quad (6)$$

显然, 只要能获取军事通信网内各指挥所的话音、数据和视频业务的用户分布、各指挥所间的吸引系数以及来话和去话业务比例, 就能计算  $S_{ij}$ 。将公式 5 作为公式 2 的比例关系式, 那么由公式 5 求得的关系矩阵则称之为业务量比例关系矩阵, 如果再知道各业务全网用户峰值平均业务量强度  $P$ , 由比例关系矩阵乘以各业务全网用户峰值平均业务量强度就可很方便地求出各业务的业务流量矩阵。

## 4 军事通信网业务流的模拟

业务流量矩阵从宏观上反映了军事通信网保障范围内各指挥所间的业务种类、强度和流向, 但还没有体现出话音、数据和视频各业务源之间的区别和特性, 为建立准确的业务流输入模型, 还应针对各业务的特性, 分别进行模拟, 以作为军事通信网作战仿真时的业务流输入模型。

### 4.1 话音业务流模型

由于各指挥所的话音用户数有限, 并且任一节



点在任一时刻的话音业务流的呼叫率与正在通话的用户数有关,正在呼叫的用户不会再提出呼叫请求。因此,军事通信网各指挥所的话音业务流为简单后效流,可近似看成是受指挥所话音用户数影响的简单后效流的全利用度系统,在任一时刻的话音业务流呼叫率正比于空闲话音用户数,其呼叫率表示为:

$$\lambda_i = (n-i) \times \lambda' \quad (7)$$

上式中,  $n$  为指挥所话音用户数,  $i$  为正在进行通话的话音用户数,  $\lambda'$  为空闲话音用户的呼叫率,另设  $N$  为节点的中继电路数。显然,当正在通话的指挥所用户数等于中继电路数后,后续的话音用户发出的呼叫将被拒绝,因此军事通信网同时也是一个呼损系统。根据话务理论可知,军事通信网的话务特性服从恩格谢特分布,其简单叙述如下:

设话源数  $n$  大于或等于线束容量  $N$  ( $n \geq N$ ), 公式 7 中  $i$  的取值范围为

$$0 \leq i \leq N \quad (8)$$

又设  $\lambda'$  为空闲话音用户的呼叫率,  $t_m$  为平均占用时间,则系统线束占用状态的概率分布服从恩格谢特分布:

$$p_i = \frac{\binom{n}{i} (\lambda' t_m)^i}{\sum_{k=0}^N \binom{n}{k} (\lambda' t_m)^k} \quad (9)$$

在式 9 中,  $i=N$ , 可以得到时间阻塞概率为:

$$E = \frac{\binom{n}{N} (\lambda' t_m)^N}{\sum_{k=0}^N \binom{n}{k} (\lambda' t_m)^k} \quad (10)$$

利用时间阻塞概率,不难推出:当  $N$  条线束繁忙时,其来话率为所有线束都空闲时的  $(n-N)/n$  倍。于是可以推导出有限信源的呼损概率

$$E' = B = \frac{\binom{n-1}{N} (\lambda' t_m)^N}{\sum_{k=0}^N \binom{n-1}{k} (\lambda' t_m)^k} \quad (11)$$

对比公式 10 和 11 可以看出,按时间计算的呼损  $E$  在数值上等于  $(n+1, A, N)$  线束的按呼叫计算的呼损率。这个关系可以用下面的式子表示:

$$E(n, A, N) = E'(n+1, A, N) \quad (12)$$

利用恩格谢特呼损表(见[1]中第 435 页),只需知道话源数  $n$ 、流入话务量  $A$ 、线束数  $N$  和有限信源的呼损概率  $B$  四个量中的任意三个就可以从表

中查到第四个量。在军事通信网作战仿真中,根据话音业务量矩阵,已知话音用户数、流入话务量和针对不同优先级用户的呼损概率,在网络规划时就可通过线束数与单路带宽的积初步确定带宽分配。

## 4.2 数据业务流模型

目前,军事通信网的数据业务流广泛采用 ON-OFF 模型,即开/关模型,它是一种常用来描述最坏突发业务的模型,其单突发源模型描述如下:

ON-OFF 模型是一般调制确定过程的一个特例,具有一个开状态和一个关状态,在任何一个活跃期,数据以固定时间间隔  $T$  发出,而在静止期,则无数据发出。本模型可以用在连续时间域或离散时间域中,这是由时间轴是离散的还是连续来决定的,活跃期和静止期的持续时间则分别服从均值为  $1/a$  (活跃期) 和  $1/b$  (静止期) 的几何分布和负指数分布。图 3 描述了开/关模型的忙期、闲期及传输数据的产生情况。

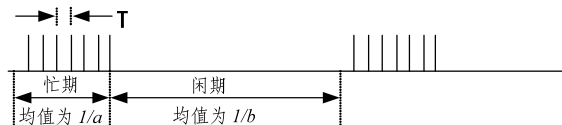


图3 开/关业务流模型

为了描述多数据业务源模型,可做如下假设:每个数据业务源的到达均符合到达率为  $\lambda$  的泊松分布,根据泊松流具有可加性,则多个数据业务源的相加仍是泊松流。

## 4.3 视频业务流模型

本文使用分形更新点过程的叠加模型<sup>[2]</sup>来产生基于分组的自相似视频业务流,它由  $M$  个广义平稳随机的分形更新点过程叠加构成,其中每个分形更新点过程由下述能量谱概率密度函数体现其到达时间间隔:

$$p(t) = \begin{cases} rA^{-1}e^{-rt/A} & 0 \leq t \leq A \\ re^{-r}A^r t^{-(r+1)} & t > A \end{cases} \quad (13)$$

式中  $1 < r < 2$ 。分形更新点过程的叠加模型中的三个参数  $(r, A, M)$  与所建立的自相似视频业务流模型中的三个参数  $(\lambda, H, T_0)$  的关系如下:

$$H = (3-r)/2,$$

$$\lambda = Mr[1 + (r-1)^{-1}e^{-r}]^{-1}/A, \quad (14)$$

$$T_0^\alpha = 2^{-1}r^{-2}e^{-r}(r-1)^{-1}(2-r)(3-r)[1 + (r-1)e^r]^2A^\alpha$$

式中， $\alpha=2-r$ 。自相似视频业务流发生模型的有限状态机具有如图 4 所示的两个状态：“init” 状态获得参数  $(\lambda, H, T_0)$ ，根据公式 14，就能分别计算出分形更新点过程的叠加模型的参数  $(r, A, M)$ ；“spawn” 状态扩展为  $M$  个分形更新点过程子过程，每一子过程代表一个独立的具有整形参数  $r$ 、位置参数  $A$  的分形更新点过程。每个分形更新点过程的有限状态机如图 5：在 “init” 状态，该过程从父过程获得相关的信息如  $r$  和  $A$ ；在 “create” 状态，将按照公式 13 中定义的间隔时间分布产生各分组。

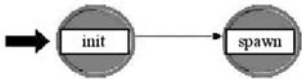


图 4 自相似视频业务流模型的有限状态机

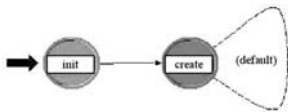


图 5 分形更新点过程的有限状态机

上述自相似视频业务流模型能比较好地体现视频业务流的突发性和相关性，同时，在多个视频业务进行叠加时，合成过程仍具有自相似性，其自相似参数与独立输入源过程中自相似参数最大值相近，合成视频业务流分组平均到达速率为各独立视频业务流的分组平均到达速率之和<sup>[3][4][5]</sup>。

4.4 指挥所业务流合并模型

军事通信网在对各指挥所进行通信保障时，通常以指挥所为单位进行整体综合保障。因此，必须对各指挥所的所有通信业务流进行模拟分析，利用网络仿真软件平台 OPNET，对各主要指挥所为单位的各通信业务流合并建模，其基本模型如图 6 所示。

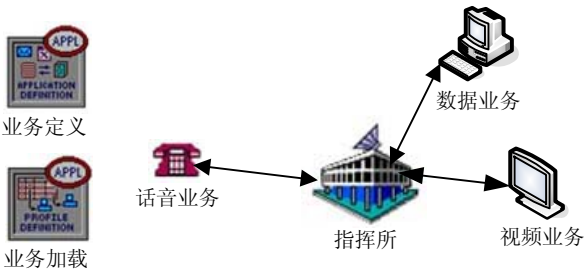


图 6 指挥所通信业务流合并模型

在业务定义模型中，对话音、数据和视频业务的单个业务源建模，即设置各业务流模型相关参数；在业务加载模型中，根据各业务的业务流量矩阵，分别描述各业务的叠加模型，从而建立了以用户（终端）群为单位的指挥所通信业务流合并模型。

5 军事通信网作战仿真实现

以下为利用 OPNET 通信网仿真软件，对某军事通信网作战运用的仿真拓扑结构模型及相应业务流加载后，在不同峰值平均业务强度仿真得到的全网平均信道利用率、语音传输时延、语音阻塞率和信元丢失率的变化情况，如图 7、8、9、10 所示。

由上述仿真结果可见，信道利用率随着业务强度的增加不断提高，在业务强度三最高时达到 80%；语音业务的平均时延随着业务强度的增加，其平均时延在增长，大约分别为 2ms、4ms 和 9.2ms，符合语音业务对时延的传输要求；语音业务的全网平均阻塞率在三种业务强度下，阻塞率大约分别为 1%、3%和 8%；数据和视频业务在三种业务强度下，信元丢失率很小，由于信道未改变，其信元丢失率基本保持不变，大约为 0.0000025%。

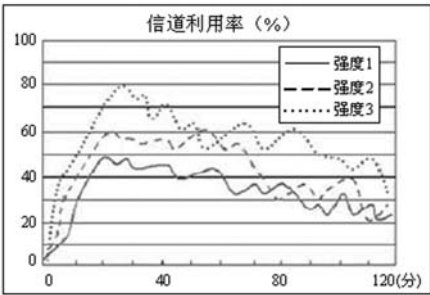


图 7 信道利用率随业务强度的变化

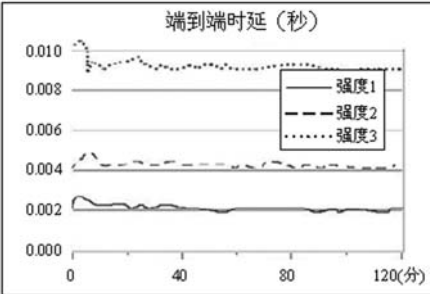


图 8 语音平均时延随业务强度的变化

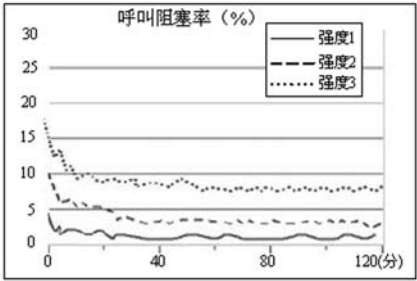


图9 呼叫阻塞率随业务强度的变化

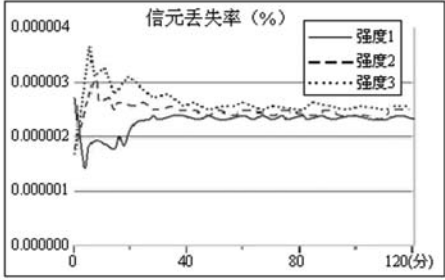


图10 信元丢失率随业务强度的变化

由以上仿真得到的网络性能参数可知，该军事通信网的组织运用方案基本能保障指挥所对各类通信业务的需求，能适应和满足作战的要求。

## 6 结束语

针对军事通信网作战仿真领域，基于吸引系数法，以通信业务流模拟为主线，分别建立了话音、数据和视频业务流模型，以此为基础进一步建立指挥所通信业务流模型，并利用 OPNET 对某军事通信网的作战运用进行仿真示例，探索了利用仿真法通过网络相关性能的定量分析以科学指导军事通信网运用的设计、规划与优化的具体方法，其基本思路 and 实现技术为科学指导军事通信网的设计和战场运用提供了有益的探索。

## 参考文献

[1] 叶酉荪. 军事通信网概论[M]. 武汉: 湖北科技出版社, 1997.

[2] B.Ryu and S. Lowen. "Fractal Traffic Models for Internet Simulation" [C].IEEE Symposium on Computers and Communications (ISCC), Juan-Les-Pins, France, 2000.

[3] A. Feldmann. "Dynamics of IP Traffic: A study of the Role of Variability and the Impact of Control"[C]. Proc. ACM SIGCOMM, Boston, 1999.

[4] Erramilli A, Roughan M. Self-similar traffic and network dynamics [J]. Proceedings of the IEEE, 90 (5), 2002:800-819.

[5] 沈宇, 徐启建, 钟静月.自相似业务流建模及其合成性能分析[J].通信学报, 25 (4), 2004:98-105.

## 作者联系方式

通信地址: 湖北武汉通信指挥学院 20 队  
邮政编码: 430010  
联系电话: 13018314096

# 数字化维修技术在陆军航空兵部队应用的初步设想

宋奕 张刚 郭鹏

**摘 要:** 数字化维修是一种面向未来的全新的航空维修思想理论, 它将现代信息技术引入到航空维修领域, 是对传统航空维修思想的发展。本文首先从分析数字化战场的基本思想及关键技术入手, 在此基础上研究数字化维修, 通过数字化战场与数字化维修的类比, 给出数字化维修的概念, 再进一步介绍数字化维修的相关技术, 借鉴并结合我陆军航空兵(以下简称陆航)机务维修本身的某些特性, 初步设想数字化维修技术在军事领域的应用。

**关键词:** 直升机; 数字化维修; 信息化; 维修信息网络

## 1 绪论

### 1.1 数字化维修概述

#### 1.1.1 数字化维修概念

传统的航空维修思想经过几十年的发展, 形成了诸如定时维修、视情维修、状态监控等理论与技术, 而数字化维修是一种面向未来的全新的航空维修思想理论。通过对维修的目标、实施过程、保障等方面的研究, 可以定义数字化维修的基本概念。

所谓数字化维修, 就是将数字化技术引入到维修领域, 将各种维修信息, 如直升机状态、诊断结果、维修资源、人力配置、备件服务、制造厂商/供应商技术支援等方面的文字、图表、语音等传统信息形式转换为数字信息, 并综合运用计算机技术、数字通信技术、网络传输技术、检测和诊断技术、多媒体技术和智能化技术, 将相关的功能系统(维修单位、航空装备管理及使用部门、制造商、装备检修部门、机组人员、有关专家、相关科研院所、其他相关部门等)有机地连成一体, 使各种数字信息能实时或近实时地传递、处理、存储与交流, 达到整个维修体系范围内的信息资源共享, 最终实现直升机维修的诊断、监控、决策、通信、保障高度一体化<sup>[1]</sup>。

总之, 就是由错综复杂的各种关于维修的“信息流”来运作“能量流”和“物质流”, 全面提高航空装备的维修能力。

#### 1.1.2 数字化维修的目的和意义

从总体上看, 数字化维修的目的和意义在于提

高维修能力和维修效率, 降低维修成本, 具体有三点。

1) 数字化维修用现代电子信息系统提高整体维修能力, 它综合所有功能体的信息, 在正确的地点、正确的时间, 提供正确的信息, 增强维修决策能力。

2) 使与维修相关的功能体(维修单位、航空装备管理及使用部门、制造商、装备检修部门、机组人员、有关专家、相关科研院所、其他相关部门等)在远距离故障诊断和维修中能够综合利用所有信息, 并通过信息共享, 大大增强协作能力。

3) 通过不断更新各种动态信息以增强状态实时感知能力, 从而减少延误和决策失误, 达到以较少的投入获得较好的成效。

#### 1.1.3 国内外数字化维修的发展状况

数字化维修是一个全新的课题, 从理论到方法目前仍处于探索阶段。

国外的一些航空业较为发达的国家在数字化维修的研究方面起步较早(从上个世纪 90 年代开始, 空中客车公司就开始数字化维修领域的研究探索), 目前已有一些成功的应用案例, 如: 空中客车公司的数字化排故及维护管理软件 AIRMAN; 美国陆军“长弓—阿帕奇”直升机(AH—64D)数字化维修系统; 美军联合攻击战斗机 JSF 采用的预测与状态管理系统(PHM)等。

我国的数字化维修研究还处于起步阶段, 与国外的发展相比还有一定的差距。国内的民航和空军对数字化维修技术比较重视, 正加紧对这一理论的研究和应用, 并取得了一定的成果。我军陆航还处于起步阶段, 在这一领域的研究相对滞后。

数字化维修是一项系统工程,需要大量的研究实践工作,需要高层领导的重视和资金的保障,需要各部门的协同配合等等。目前各相关部门正逐渐认识到数字化维修对提高航空维修效能的重要作用,并正加紧对这一领域的研究,相信我国的数字化维修思想和技术将有更进一步的发展。

## 1.2 将数字化维修技术应用于陆航机务维修的目的和意义

数字化维修就是在维修工作中,充分利用数字化技术,借助各种信息平台,对直升机进行实时状态监控,对维修资源实现优化管理与共享,对维修技术实现远程信息支援。数字化维修将给传统的维修模式带来革命性的变化,随着数字化维修系统的发展、完善和应用的深入,将改变人们传统的维修观念、维修方式。数字化维修是一种手段,是对现代化维修技术的完善、补充和提高,其最终目的是提高直升机的完好率和战斗恢复率。

## 2 数字化维修技术在我军陆航部队应用的初步设想

数字化维修是一个全新的课题,我军在这一领域的研究还处于探索阶段。

数字化维修就是在维修工作中,充分利用数字化技术,借助各种信息平台,对直升机进行实时状态监控,对维修资源实现优化管理与共享,对维修技术实现远程信息支援。数字化维修的目的是提高维修效率,即保证维修效果,缩短维修时间。

目前,通常采用的维修方式是基于装备状况的视情维修和基于时间的定时维修,相比数字化维修方式,它们不利于:缩短维修和供应保障过程、减少使用和保障费用、提高直升机的出动架次率。另外,数字化技术在新型装备上应用程度的不断提高已是一个必然的发展趋势,传统的维修方式将无法适用于未来的航空机务维修工作。这些情况都说明了在陆航机务维修工作中引入数字化维修思想的重要性和必要性。

由于数字化维修是一个全新的课题,从理论到方法目前仍处于探索阶段,所以本文将结合数字化维修的特点,借鉴并结合我军陆航机务维修本身的某些特性,对数字化维修技术在我军陆航部队的应

用进行初步的设想。

### 2.1 陆航数字化维修的应用前景

传统的维修方式从定时维修到视情维修,再到状态监控维修,其目的都是为了追求维修效率的提高。随着信息化的发展,人们将数字化技术引入到航空维修领域,就产生了数字化维修。数字化维修是一种全新的维修方式,是对传统维修方式的发展,广泛的采用先进的数字化技术,以提高维修效率。

数字化维修的核心目的是:实现直升机维修的实时、准确、高效。下面介绍一下数字化维修技术在陆航的具体应用前景。

#### 2.1.1 IETM技术的引入

在维修过程中需要查阅各种维修手册和资料,而目前与维修相关的技术资料大多以纸张的形式存在,查阅如此之多的手册和资料,会浪费大量的时间和精力,降低了维修效率。如果将 IETM 技术引入到履历本和技术资料等纸制文本文件的管理中,就能很好的解决这一问题:使现有技术资料数字化,方便管理和保存;提供查询检索功能,方便使用;实现网络共享化,通过网络远程查询,达到远程资源共享。另外技术资料的数字化为航空维修便携式计算机 PMA 在维修工作中的应用,提供了前提条件。因为 PMA 的重要作用之一就是提供对电子技术资料的交互式查询,可以为维修工作人员在工作岗位上提供实时的维修技术资料支持,提供技术资料的交互式查询、检索以及更新,以提供部件的详细数据,缩短维修时间。

#### 2.1.2 航空维修便携式计算机PMA的应用

PMA 可以简明定义为用于维修现场的可移动计算机设备,是维修信息管理系统的重要组成部分。除了提供对电子技术资料的交互式查询外,PMA 还具有故障部件的隔离、维修监控、备件的管理、维修信息的分析、故障预测以及数据的上传与下载等功能。技术资料的数字化为 PMA 的应用提供了前提条件,同时 PMA 也为数字化技术资料的使用提供了平台,二者相辅相成,给维修人员带来极大便利。

### 2.1.3 全实时状态监控技术的应用

在现有的保障维修系统中,其相关机载设备不能在直升机飞行中自动将数据传送给地面,只有等直升机着陆后,从机上下载有关状态监控和故障诊断数据,并对飞行员所做的飞行后报告进行综合分析后,才能开始准备所需的零备件、工具和设备,指派适当的维修人员进行维修和保养。采用先进的状态监控方法与手段,实现对直升机机械、电子系统和部件的全机多传感器监测,构成了直升机数字化维修的基础性技术。利用先进的传感器实时“感知”直升机状态,对直升机进行实时状态监控;利用故障预测与状态管理系统(PHM)来预测、监控和管理直升机的状态;收集直升机故障信息,以空地数据链(ACARS)形式由空中向地面的维修信息管理系统(维修信息中心)实时传送。

### 2.1.4 构建维修信息管理系统

利用先进的计算机技术、网络技术、通讯技术和数据库技术等,构建维修信息管理系统,采集、处理、分析、管理维修信息,利用数据仓库,数据挖掘,信息融合等技术对维修信息和相关历史数据进行挖掘和分析处理,得出少冗余的维修相关信息,提供给维修管理者、维修人员、相关专家,专家系统或者提供给维修辅助分析决策系统,以形成最后的维修方案。

维修信息管理系统主要包括维修数据库和维修信息管理两大部分。

维修数据库是直升机数字化维修的基础,为直升机数字化维修系统提供基本数据,实现直升机维修信息的自动化管理,可以充分挖掘多种有用信息。主要具有以下功能:基于计算机网络,建立分布式维修数据库,实现维修信息管理自动化;具备数据挖掘功能,抽取有用信息,实现维修辅助决策;具有安全保密功能;具有较强的可扩展性和兼容性;具备初步的可视化功能,实现航材备件、仓库、人员及其他信息的可视化。

维修信息管理能够实现以下功能:能够实时查询与维修相关的各类信息,如各型号直升机的维修记录信息、技术状况、维护管理情况等;实现对装备维修保障资源(各级仓储航材备件、各种物资器材等)的可视化管理,实现对物资器材的查询、收发、调配等业务。

### 2.1.5 构建维修信息网络

装备维修信息传输,通过装备维修信息网络支持系统实现。网络支持系统是建立在全军军事训练信息网(军训网)网络平台上的一个专用网络系统,通过网络互联设备、服务器及工作站和相应的软件系统构成一个星形的网络系统,实现各级装备维修部门之间的信息共享和信息支持,是提高装备维修效率的有力工具。

该系统具有以下功能:

- 1) 构建基于全军军事训练信息网的维修信息传输网络平台,实现维修信息安全可靠地传输。
- 2) 各级维修中心实现信息共享和信息支持。
- 3) 能够实现数据、视频、音频等多媒体信息的传输和远程访问功能。
- 4) 提供多种信息传输手段,可以利用民用通信网络实现信息安全传输。
- 5) 具备信息传输安全保密功能。<sup>[2]</sup>

## 2.2 应用的初步构想——以军训网为依托构建数字化维修信息网络

信息网络是数字化维修信息传输的平台,是直升机数字化维修的基础和纽带,构建以全军军事训练信息网(简称军训网)为依托的直升机数字化维修信息网络有着十分重要的意义。

直升机数字化维修信息网络是一个以军训网为基础的专用网络系统。它采用 Internet 技术构建,实现各级维修信息中心的互联互通,实现维修信息资源共享。

### 2.2.1 直升机数字化维修信息网络的主要功能

直升机数字化维修信息网络的主要功能有:

- 1) 为陆航各级维修相关部门和人员提供专用技术保障网络。
- 2) 为各级维修技术保障信息提供高效可靠的信息传输手段。
- 3) 通过军训网实现各级维修信息中心互联互通。
- 4) 具有远程多媒体信息通信功能,可以传输视频图像、声音、数据等多种信息。
- 5) 具有稳定可靠的信息传输能力,具有有效的容错能力,接点之间具有多条路由。
- 6) 具有网络管理能力,各级维修信息中心可以实现对维修信息网络运行状态的动态监测和故障

诊断能力，能及时有效地调整、分配网络资源。

7) 具有网络安全功能，具有硬件防火墙、信息加密机制、身份认证机制，能审计跟踪重要事件。系统管理员可根据需要重新设置重要事件。具有定期或不定期的统计、分析功能，具有高效的防病毒功能。

2.2.2 直升机数字化维修信息网络的体系结构

(1) 构建陆航维修信息网

以军训网为平台构建全军范围内的陆航维修信息网，实现陆航各维修相关单位的网络连接。

维修网络信息中心负责完成网络地址分配和域名管理；负责对陆航维修信息网的全面管理；负责随时掌控各基层单位的维修信息，提供给高级维修管理部门；负责维修信息中心数据库的建设和管理；负责总部级维修信息管理系统的建设和管理；负责相关硬件和软件的基础建设，实现远程共享，为基层单位级维修信息中心提供强大的网络硬件和软件的支持；开发维修专家系统、辅助分析决策系统、维修能力评估系统、远程故障诊断系统等系统，实现对基层单位级维修信息中心的共享，提升整体的数字化维修能力。

基层单位维修信息中心负责基层单位的维修信息管理系统的建设任务和日常的信息管理工作；负责分部式维修信息数据库建设与管理；负责基层单位局域网的日常维护和信息安全工作；负责对维修信息的更新工作。陆航维修信息网体系结构见图 1。

(2) 构建基层单位内部的信息处理中心

维修信息中心是基层单位内部数字化维修信息网络的核心，由一台或多台高性能服务器和相关软件组成。

维修信息中心负责对各种维修信息的采集、处理、分析、管理，利用数据仓库、数据挖掘、信息融合等技术对维修信息和相关历史数据进行挖掘和分析处理，得出少冗余的维修相关信息，提供给维修管理者、维修人员、相关专家，或提供给维修诊断专家系统和维修辅助分析决策系统，以形成最后的维修方案。

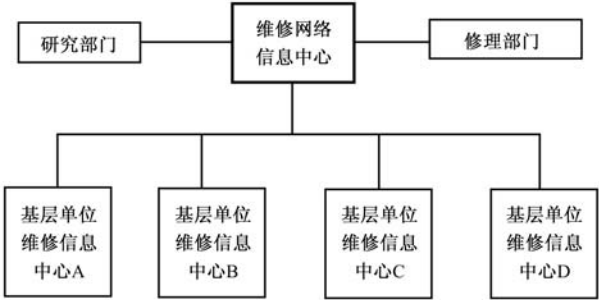


图 1 陆航维修信息网体系结构图

全机状态监控系统通过空地数据链为维修信息中心提供实时的直升机状态信息。维修信息中心为维修诊断专家系统和维修辅助分析决策系统提供相关故障信息。维修信息中心通过维修资源管理系统实现对维修资源的管理和调配。维修信息数据库为维修信息中心提供多方面的信息：状态监控信息、保障资源信息、历史数据信息、相关技术资料、其他相关维修单位提供的技术支援信息、主管部门下达的管理信息等。维修信息中心与陆航维修信息网连接，具备远程故障诊断能力。维修信息中心负责对基层单位局域网的管理和维护。基层单位局域网内设有维修机组工作站，负责向维修信息中心汇报机组的工作情况，提供维修信息等。维修信息中心结构体系见图 2。

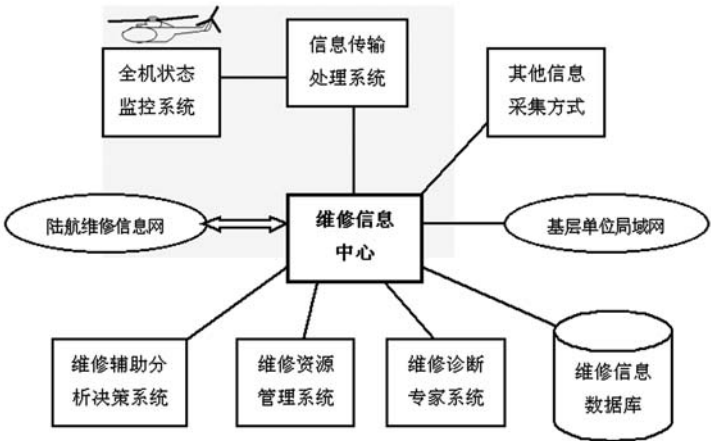


图 2 基层单位内部维修信息中心



(3) 构建基层单位内部局域网

对于基层单位内部局域网的建设，拟采用以交换机为中心的星型拓扑机构，具有简单、可靠、灵活等特点。

维修机组是直升机维修工作的具体实施者，在基层单位的局域网中为每个维修机组设立一个维修工作站，便于维修一线的机组与信息中心和维修管理部门之间的信息沟通。维修机组工作站通过交换机实现与陆航维修信息网的连接，为每名一线的机务维修工作者提供了网络信息交流的平台，通过机

务维修 BBS，可以交流维修经验，提出维修中遇到的问题供大家共同探讨并获得解答，维修中出现的失误供大家共同借鉴等。

维修现场的便携式维修计算机 PMA 可以通过无线通信连接到局域网中，共享网络信息资源，向维修信息中心提供故障信息。网络管理员负责对网络的日常管理。数据库服务器为网络提高数据库支持。局域网为维修专家设置了诊断专家工作站。局域网通过交换机、防火墙、路由器连接到陆航维修信息网。陆航内部局域网的构建方式见图 3。

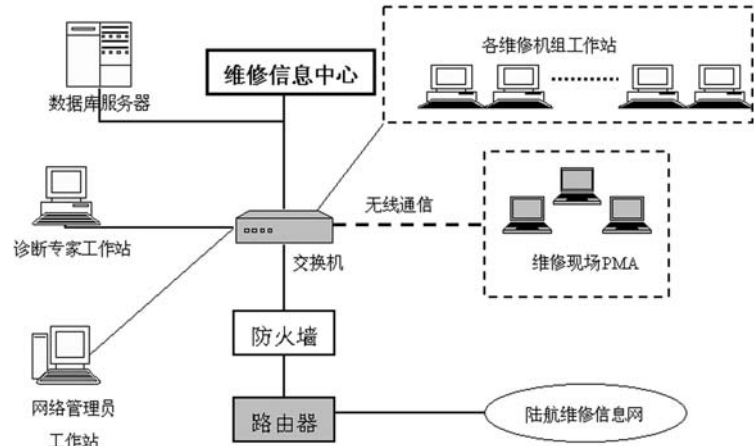


图 3 基层单位内部局域网构建方式

2.3 应注意的问题

2.3.1 应注意加强对数字化维修人才的培养

人才是直升机数字化维修中的关键因素。努力培养和造就一支适应陆航数字化维修建设需要的结构合理、素质很高的人才队伍，既是数字化维修建设的紧迫任务，又是保证数字化维修建设持续健康发展的重要保障。管理部门应制定明确的规章制度，有计划的组织各种培训，加强对数字化维修人才的培养。

数字化维修从总体上确实带来了维修的便利，但从普通维修人员的角度来看，他们首先面临的问题是学习数字化维修技术，对于其中的一些同志，这可能是非常困难的，可能会出现安于现状的想法：“现在的方法干的好好的，为什么要学习新东西，学习新东西要一个过程，用起来不熟练，还不如老办法效率高呢”。

面对新事物，站在不同的角度总是会有不同的看法，这是正常的。但如果用消极的态度来学习数字化维修技术，就是不可取的。数字化维修是对传

统维修的发展，有效地提高了维修效率。由于对数字化维修技术掌握不熟练，以及数字化维修体系发展还不完善，相关的规章制度还不健全，可能会在初期遇到这样那样的困难，反而会影响维修效率的提高。但是我们应当看到这只是暂时的，长远的看数字化维修将极大地提高维修效率，数字化维修在我军陆航部队的应用将是必然的趋势。

2.3.2 陆航数字化维修的建设原则

参考相关文献，并结合陆航数字化维修的特点，我认为陆航的数字化维修建设应遵循如下原则：

高层主导，理论先行：由高层领导挂帅，研究和创新数字化维修理论体系，引领数字化维修建设的实践。

统筹规划，需求牵引：对数字化维修建设实行统一领导、统一组织，制定总体框架，以应用需求引导和推动建设的实践。

资源共享，确保一体：加强标准化意识，实现数字化维修领域不同硬件、操作系统、数据库、应用程序之间的互联互通和信息共享。



重点突破,逐步推进:有步骤有重点地逐步建设,以重点项目的突破促进全面发展。

建用并重,保证安全:在建设中,要始终把安全保密工作放在重要位置,确保数字化维修系统安全可靠地使用。

强化创新,人才为本:在理论、技术和体制等方面进行大胆的探索和创新,把培养数字化维修人才作为一项战略工程,抓紧抓好<sup>[3]</sup>。

### 3 结论

提高维修效率是航空维修永恒的主题。

数字化维修是一种面向未来的全新的航空维修思想理论,它将现代信息技术引入到航空维修领域,是对传统航空维修思想的发展,极大的提高航空维修的效率。数字化维修技术的应用是航空业的大势所趋。

本文深入分析数字化维修技术的内涵与原则,结合我军陆航实际,初步设想数字化维修技术在我军陆航部队的应用。尤其在以军训网为依托构建数字化维修信息网络方面提出了自己的一些看法。本文的主旨在于通过对数字化维修的研究,探讨数字化维修技术在我军陆航的应用原则及方法,最终提高我军陆航部队的维修效率。

### 参考文献

- [1] 高红星,左洪福.面向未来的民航数字化维修[J].航空维修与工程,2005,(2):24-26.
- [2] 宋建社等.装备维修信息化工程[M].北京:国防工业出版社,2005.
- [3] 魏长虹,古平,李胜红,龚传信.对我军装备维修信息化的初步思考[A].见:维修保障理论与应用--中国兵工学会第二届维修专业学术年会论文集[C].北京:解放军出版社,2004.

### 作者联系方式

通信地址:北京市通州区台湖镇陆军航空兵学院机械工程系机械维护教研室

邮政编码:101123

联系电话:010-66877765

# 一种基于DDS的实时信息分发框架RIDF

王珩 丁峰

**摘 要：**实现实时信息的灵活、按需、高效分发是大型信息系统和分布式应用有效运行的关键，在数据分发服务 DDS 研究基础上，针对分布式应用系统对实时信息分发需求，提出一种基于 DDS 的实时信息分发框架 RIDF，并通过具体应用实例说明了发布/订阅过程。  
**关键词：**数据分发服务；实时信息分发；发布/订阅；框架

## 1 引言

在许多分布式应用和企业信息系统中存在着大量信息数据资源，这些资源既包括各业务领域保存的数据库数据（静态数据），也包括大量诸如实时控制、实时交易等实时信息。特别是这些实时信息，将直接关系到企业运转和系统运行的稳定性和高效性。因此，在分布式应用中如何实现实时信息的按需分发是当前研究人员关注的热点问题之一。

针对分布式系统的实时应用和信息分发问题，OMG 组织于 2004 年发布了第一个实时、数据中心思想的发布/订阅通信范型——数据分发服务（Data Distribution Service, DDS）规范<sup>[1, 2]</sup>。DDS 面向网络中心环境，实现分布式实时应用在灵活传送需求和动态组网条件下，向多个节点的快速分发。本文在 DDS 规范研究基础上，针对信息系统和分布式应用对实时信息分发的需求，提出一种基于 DDS 的实时信息分发框架 RIDF。

## 2 DDS概述及其应用

DDS 是 OMG 公布的发布/订阅（Publish/Subscriber, PS）数据分发系统规范，它定义了以数据为中心的发布/订阅（Data-Centric Publish Subscriber）机制，提供了一个与平台无关的数据模型，以简化分布式系统中数据的有效发布，它主要应用在要求高性能、可预见性和对资源有效使用的关键任务领域。

DDS 遵循发布/订阅分发模型<sup>[3]</sup>，通过发布/订阅连接匿名信息提供者（发布者）和信息使用者（订阅者）。DDS 规范的主要实体包括：发布者、

数据写入者、订阅者、数据读取者、主题以及域参与者。整个分布式应用由参与者进程组成，这些进程运行在不同计算机上的不同地址空间内。参与者可以同时发布和订阅由“主题”标识的数据流（信息）。参与者能通过 DDS 提供的标准 API 接口有效而简单地“读”和“写”数据。实际上，该服务创建一个全局“数据空间”以便任何参与者都能读取和写入。DDS 体系结构的概念示意如图 1 所示。

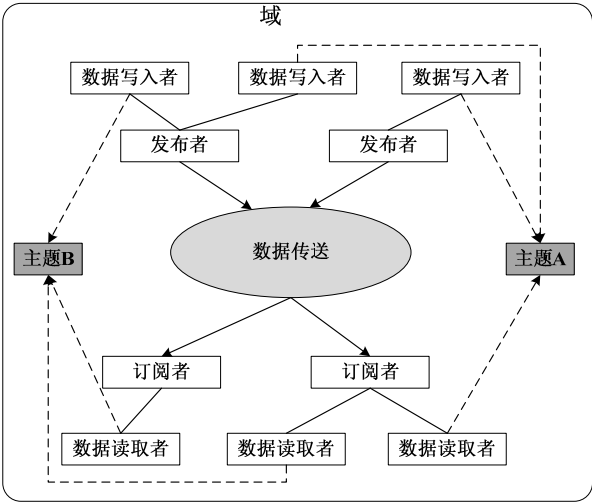


图 1 DDS 体系结构概念示意图

DDS 是一个通用的数据分发规范，以一种纯数据中心交换模式进行应用之间的通信。DDS 着眼于以数据为中心的分布式实时系统，具有松散耦合、处理复杂数据流能力强、分发效率高、容错性好以及动态可配置等特点。因此，DDS 强大的功能和良好的性能使其在工业自动化、分布控制与模拟、电信设备控制、传感器网络、网络管理系统、C<sup>4</sup>I 军事领域等各个领域的实时系统中已得到了广泛的应用，具体包括<sup>[4, 5]</sup>：

- 1) 海上高级平台控制系统（APCS）—海上

- SLICE 中的消息传送采用 DDS 机制进行；
- 2) DDS 为日本东京高速公路流量监控系统和美国火车运行管理提供实时流量监控信息传递的支持；
  - 3) 美国爱荷华州大学的驾驶模拟器 (Driving Simulator)、以及美军飞行和舰船模拟器中的实时数据交换和共享均采用 DDS 规范；
  - 4) DDS 还在谐波数字电视视频点播和 IP 电话等电信级业务和系统中得到广泛应用；
  - 5) 此外，2004 年 7 月，美国国防部 DoD 国防信息系统局 DISR 选择 DDS 作为其 GIG 的发布—订阅标准，并被纳入美军的联合技术体系结构 JTA 中，成为 DoD 的一项重要标准；DDS 美陆军的未来作战系统 FCS 项目和美海军的一些系统中的通信传输和数据分发方面得到成功应用。

3 基于DDS的实时信息分发框架RIDF

3.1 信息系统和分布式应用对实时信息分发的要求

在大型信息系统和分布式应用中，大量实时信息存在于提供信息的各个成员系统中，它们以信息流和数据存储的方式提供给信息用户使用，这些信息和数据流复杂，信息分发关系根据战场需要包括一对多，多对一和多对多。而且，信息的分发还需要满足按需、实时性、可靠性、容错性、动态配置、可扩展性等要求。具体包括：

- (1) 按需分发  
在分布式应用和信息系统中，应根据用户需要，建立灵活的信息分发机制，在大量信息存在的情况下实现信息灵活、按需的分发。
- (2) 实时性  
由于实时信息将直接关系到系统的运行控制和有效运转，因此需要在很短的时间内（通常为几秒）传送到用户那里。
- (3) 高效性  
在网络环境中，用户种类繁多，通常信息需要同时发送到多个用户那里，直接使用单播或广播模式往往会占用大量带宽且传送效率低。因此，实时信息分发需要组播支持，这样既保证一份数据能同时发往多个用户，又保证网络中任何一条链路上只传送单一的数据包，从而节省网络带宽、提高数据传送效率，减少网络拥塞的可能性。
- (4) 基于服务质量和策略的分发  
鉴于实时信息的重要性，在进行实时信息分发时，不仅要保证信息的快速分发，同时还要对信息的可靠性、持久性、丢报率、传送优先级等 QoS 属性予以保证，甚至需要控制管理人员对分发进行策略管理和人工干预，从而确保重要信息在一定带宽条件下，一定时间内优先传送。

3.2 基于DDS的实时信息分发框架

基于上述需求，结合 DDS 规范的特点，本文给出了一种基于 DDS 的通用实时信息分发框架——RIDF (Real-time Information Dissemination Framework based on DDS)，如图 2 所示。

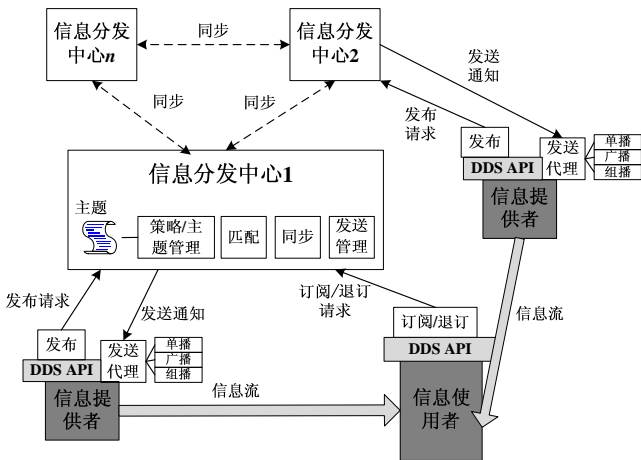


图 2 基于 DDS 的实时信息分发框架 RIDF

在 RIDF 中，参与的实体包括信息提供者、信息使用者和信息分发中心。其中：

1) 信息提供者调用 DDS 接口进行基于主题的信息发布，同时通过发送代理监听来自信息分发中心的发送通知，将信息发送给指定信息使用者，发送方式包括单播、广播和组播。

2) 信息使用者调用 DDS 接口进行信息订阅/退订。

3) 信息分发中心接收信息提供者的信息发布请求以及信息使用者的订阅请求，并提供信息匹配、管理、同步、发送通知等功能。信息分发中心可以有多个，按照具体分布式应用特点的进行部署，如分层分级等。

信息分发中心提供的具体功能包括：信息分发中心收到订阅请求后，通过匹配确定有哪些提供者提供了订阅的信息，并通过发送管理模块通知信息提供者；策略/主题管理对分发策略、信息分发的 QoS 以及信息主题进行维护和管理，提供策略（按照信息优先级或网络资源情况）和服务质量的制定和编辑功能，策略管理模块还支持根据信息的重要性由管理人员决定强制将某些信息推送给特定用户；同步模块实现不同信息分发中心信息产品的实时/准实时同步。

3.3 应用实例

本节通过一个简单的实例来说明应用 DDS 如

何进行实时信息发布、订阅以及如何得到信息。假设信息提供者是高速公路流量监控服务端，它具有实时监控信息需要发布。监控中心需要这些实时信息进行显示和管理，对其进行订阅。本文给出信息提供者端的发布过程、信息使用者端的订阅过程以及信息获取过程的程序序列图，如图 3 所示。

发布者端程序进行信息发布的过程为：

1) 域参与者创建发布者：publisher=domain->create\_publisher (...);

2) 域参与者创建主题：topic=domain->create\_topic (“车流量信息”，“监控信息”，...);

3) 发布者创建数据写入者：

  DataWriter writer=publisher->create\_datawriter (topic, ...);

  AppDataWriter appwriter = AppDataWriter::narrow (writer);

4) 应用写入数据，例如：TrafficMonitorInfo; appwriter->writer (&TrafficMonitorInfo);

订阅者端进行信息订阅的过程为：

1) 域参与者创建订阅者：subs = domain->create\_subscriber (...);

2) 创建感兴趣的主题：topic = domain->create\_topic (“车流量信息”，“监控信息”，...);

3) 创建数据读取者监听接口：AppListener reader\_listener = new AppListener ();

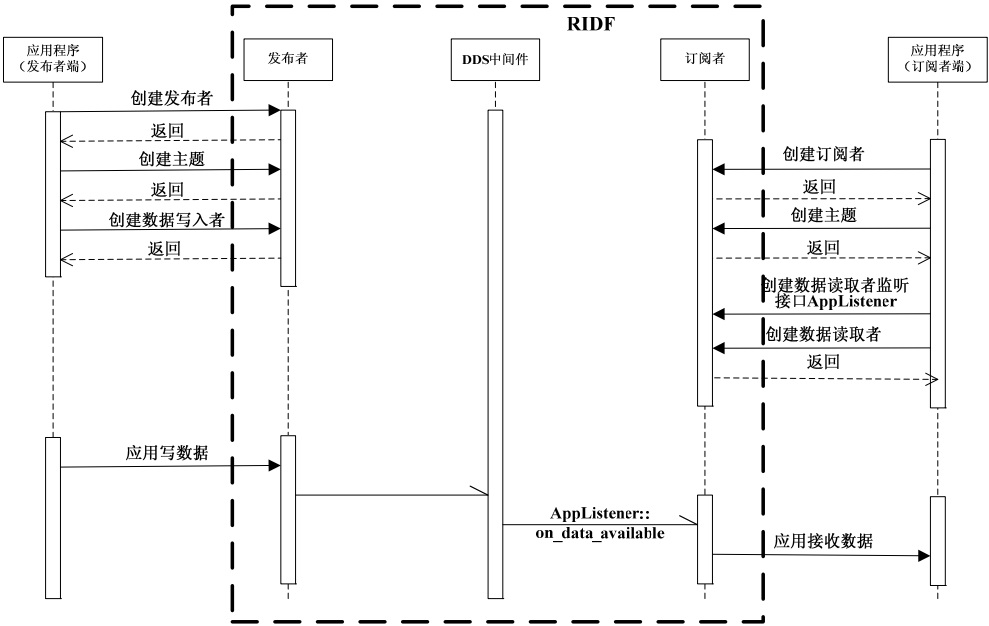


图 3 基于 DDS 的发布/订阅过程序列图

4) 订阅者创建数据读取者, 并关联至 Listener:

```
DataReader reader = subs->create_datareader  
(topic, ..., reader_listener, ...);
```

当接收到订阅的信息, 会自动回调数据读取者监听接口 `reader_listener` 的 `on_data_available` 方法通知订阅者, 订阅者获得信息并进行相应处理。

中基于发布/订阅模式的数据分发提供了有效的解决途径和规范支撑。本文结合分布式信息系统实时信息分发的需求, 在 DDS 规范研究基础上, 提出一种基于 DDS 的通用实时信息分发框架。该框架充分利用 DDS 的特点, 提供通用、灵活、高效的实时信息分发机制, 为应用领域构建实时信息分发系统提供了技术支撑。

## 4 结论

OMG 组织公布的 DDS 规范为实现分布式系统

## 参考文献

- [1] OMG. Data Distribution Service for Real-time Systems Specification version 1.0. OMG, Dec. 2004. OMG Technical Document.
- [2] G. Pardo-Castellote. OMG Data-Distribution Service: Architectural Overview. In Proceedings of the 23<sup>rd</sup> International Conference on Distributed Computing Systems Workshops (ICDCSW'03), 2003.
- [3] R. Rajkumar, M. Gagliardi, and L. Sha. The Real-Time Publisher/Subscriber Inter-Process Communication Model for Distributed Real-Time Systems: Design and Implementation. In Proceeding of the 1st IEEE Real-Time Technology and Applications Symposium, Denver, Colorado, USA, May 1995.
- [4] G. Pardo-Castellote. DDS Spec Outfits Publish-Subscribe Technology for the GIG. COTS Journal, 2005, 4.
- [5] RTI. The Data-Centric Future. The Real-Time Middleware Company, 2007.

## 作者联系方式

通信地址: C<sup>4</sup>ISR 技术国防科技重点实验室 (28 所分实验室)

邮政编码: 210007

联系电话: 025-84288513

# 基于裁剪超宽带MAC协议的无线传感器网络

王延峰 李林

**摘 要：**无线传感器网络集成无线网络通信，嵌入式处理，微型传感器制造等多项技术，是传感器发展的一个趋势。文章对现有应用于无线传感器网络的各类型的介质访问控制协议进行了简要分析，进而提出把裁剪超宽带介质访问协议应用于无线传感器网络并对这种协议进行了可行性分析。

**关键词：**无线传感器网络；介质访问控制协议；超宽带；裁剪超宽带协议

无线传感器网络（wireless sensor network，WSN）是由多学科高度交叉的新兴前沿热点研究领域。无线通信技术、信息处理和传输为基础的无线传感器网络提供了有力的技术支持。无线传感器网络扩展了人们的信息获取能力，将客观世界的物理信息同传输网络连接在一起，在下一代互联网中将为人们提供最直接、最有效、最真实的信息。

## 1 引言

无线传感器网络的一个重要特征就是低功耗、低成本和小体积。无线传感网络研究的核心问题之一就是功耗管理。传统的正弦载波通信由于存在中频、射频等电路难以达到无线传感器网络的低成本要求，同时正弦载波通信的固有组成部分为降低成本、减少体积带来了阻碍。射频模块是最大的耗能模块，是优化的主要目标。介质访问控制（medium access control，MAC）协议直接控制射频模块，对传感器节点功耗有很大影响。超宽带无线电 UWB（Ultra wideband radio）是近年来发展迅猛的新型通信方式，它是基于冲激脉冲（纳秒级窄脉冲）自身的宽频特性，通过对其特殊波形的冲激脉冲进行调制获得载有信息且符合频带要求的无线电信号，即所谓超宽带冲激无线电<sup>[1]</sup>。超宽带无线电直接发射脉冲，无须中频和射频电路，对于减小体积和降低能源消耗具有特别的意义，尤其适合微小传感器节点的设计。同时超宽带无线电还具有空间传输容量大、对多径的分辨能力高、功率谱密度低、信号隐蔽性好等优点能够很好地满足密集型传感器网络的要求。当前，国内外对无线传感器的研究大都是利用传统正弦无线电通信作为传输手段，

只有美国方面启动了“超宽带无线传感器网络”。由于超宽带无线电应用于无线传感器网络能解决若干传统正弦无线电难以解决的问题，具有特别明显的优势。超宽带无线电传感器网络的研究和开发势必成为必然。

## 2 无线传感器网络MAC协议进展

在无线传感器网络中，介质访问控制（MAC）协议决定无线信道的使用方式，在传感器节点之间分配有限的无线通信资源，用来构建传感器网络系统的底层基础结构。目前，所了解的无线传感器网络 MAC 协议中，基于冲激脉冲通信的 MAC 协议甚少，都是基于正弦载波通信的 MAC 协议。对于传统无线传感器网络 MAC 协议有如下三种分类（参见表 1）。

表 1 传感器网络 MAC 协议对比

MAC 协议	描 述
SMACS, EAR	固定时隙收发数据，在空闲时将节点转入休眠状态以减小能耗
组合 TDMA/FSMA	选择适宜数量的信道，在相应中心频率信道内时分复用
基于 CSMA 介质访问	基于竞争机制随机接入，通过调整相位避免冲突重复发生

1) SMACS（Self-Organizing Medium Access Control for Sensor Networks 自组织传感器介质访问控制）和 EAR（Eavesdrop And Register 窃听登记）：SMACS 实现网络启动和链路层组织，EAR 算法完成移动节点和传感器网络的无缝连接。SMACS 是节点不需依靠主控中心能够独立进行邻

居节点发现、建立并维护表中一的自组织分布式网络底层基础协议,这种协议将邻居发现与信道分配有机地结合起来。EAR 是对 SMACS 引入了移动节点。网络模型依然呈静态性即每个移动节点对临近的静态点负责。这种时隙分配机制的不足在于当节点属于不同子网时有可能无法建立连接。

2) 组合 TDMA/FDMA: 根据射频传输消耗的能量来优化选取信道的数量.当用于发送消耗能量过多时趋于 TDMA 工作方式,而在以接收为主要能量消耗时更趋向于 FDMA 工作方式。

3) 基于 CSMA (Carrier Sense Multiple Access 载波侦听多址接入) 法: 任何 CSMA 框架由侦听机制和退避机制两个主要部分组成。传统的 CSMA 是在随机分布传输假设基础上趋向于独立的点对点数据流。针对传感器的 MAC 协议必须能够提供数量可变的、高度相关的、定期占支配作用的数据流。一种自适应传输速率控制 (ARC, adaptive transmission rate control) 的方法被提出来平衡源发起与数据流通的速率,这种计算特性相比消息握手机制更为能量高效,而且试图通过不断调整传输速率和改变相位避免冲突的重复发生。

### 3 研究超宽带无线网络MAC协议的意义

设计一个无线传感器网络的 MAC 设计主要应该考虑到以下性能指标,一是能源有效性,另一个是可扩展性,协议要能自动适应网络大小,节点密度和拓扑结构的变化,其他一些性能指标包括:信道访问的公平性、延迟、吞吐量、带宽利用率等。传统 MAC 协议中首要考虑的性能指标在无线传感器网络中和前两个性能指标中,其重要性次之。

UWB 与传统的窄带或其他宽带通信技术相比,有两个主要特点。

1) 频带宽,功率谱密度小。UWB 系统的带宽超过中心频率的 25%或者超过 1.5G Hz.明显宽于当前通信系统所用的带宽。其主要的工作频带被限制在 3.1-10.6G Hz,功率谱密度将被要求低于 -41.3dBm/M Hz。由于脉冲的超短持续时间,使得 UWB 系统具有重要的内在优势对抗多径衰落。

2) 无载波方式。典型的 UWB 以一种无载波的方式实现,可以直接调制非常尖锐的脉冲,从而导致波形占用几个 GHz 的带宽。因此不需要本地

生成载波, UWB 发射器直接用脉冲波形激励天线,不需要传统收发器所需的变频,从而不需要功率放大器和混频器,允许采用非常低廉的宽带发射器。同时,在接收端, UWB 接收机也有别于传统的超外差接收机,不需要中频处理,不必提供多级混合电路、成形滤波等。因此, UWB 收发器的电路结构比传统收发器简单。

因此,超宽带在无线传感器中的应用成为一种不错的方案。

## 4 裁剪UWB MAC协议在无线传感器网络应用

### 4.1 裁剪UWB MAC协议介绍

非对等 (Uncoordinated)、无线 (Wireless)、低等级 (Baseborn) 介质访问 UWB 通信网络 (UWB)<sup>2</sup> 协议<sup>[2]</sup>在 UWB 系统的特定情况下应用多码 (Multi-code) 概念,采用基于公共控制信道和数据信道的混合方案,公共控制信道由公共 TH 码提供,数据信道与发射机码相联系。混合方案采用的可阐述如下。

1) 由于数据发送 (与相应的 TH 码) 首先在控制信道上通信,简化了接收机结构。

2) 提供了用于广播的公共信道。例如路由和分布式定位协议等是需要广播信息的。

至于码分配,MAC ID 与发射机码之间的唯一性可通过采用<sup>[3]</sup>中描述的算法获得。其码的产生是基于 MAC ID,避免了实行分布式码分配协议。

由于每个终端存在时钟漂移, (UWB)<sup>2</sup> 没有假设开始发送包时发射机与接收机是同步的。因此,包中所加的同步头应足够长以保证所需的同步概率。同步头的长度与网络当前状态有关并由同步逻辑提供给 MAC。

(UWB)<sup>2</sup> 也使用 UWB 提供的测距能力。发射机与接收机之间的距离信息在控制包交换期间收集。这种信息可以使 MAC 的多个特性得以优化,并允许新功能的引入,比如分布式定位。

### 4.2 (UWB)<sup>2</sup>在无线传感器网络中仿真

仿真方案组成 N 个终端,随机分布在  $80 \times 80 \text{m}^2$  尺寸的面积上。每个终端特征是,有保

证在终端之间整个连通的无线电，无线电发送距离为 200m。在网络中每个终端生成 MAC 服务数据单元 MACPDU 并发送到其他终端，遵从平均相互到达时间  $T_{PDU}$  的泊松过程。每个 MACPDU 的尺寸设为  $L=2000b$ ，根据 UWB 物理层参数脉冲传输率设为  $1Mb/s$ 、 $N_s=1$  和  $T_p=1ns$

在仿真中，我们假定所有终端采用相同同步序列。

$(UWB)^2$  协议的性能被估算，终端数量在 25 到 100 之间变化，并且有三个不同  $T_{PDU}$  值：2.5s、1.25s 和 0.3125s 分别对应的数据传输率为 800b/s、1600b/s 和 6400b/s。

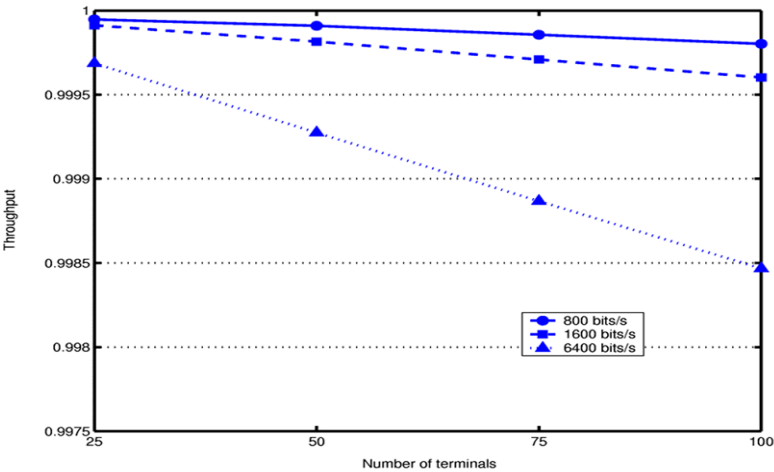
分组错误概率  $Pr_p$  的计算，没有考虑分组的纠错能力，并假设分组中所有比特正确时分组才正

确。仿真过程中，采用实时评估的活动用户数  $N_U$  来计算脉冲碰撞概率。 $Pr_p$  由修正后的 (1) 式来估计，强调了  $Pr_p$  对  $N_U$  的信赖性，也反应了比特与比特间的不同。

$$Pr_p = 1 - \prod_{i=0}^{L-1} (1 - Pr_b(i)) \tag{1}$$

这里的  $Pr_b(i)$  是数据分组中的第  $i$  比特的错误概率。

$Pr_p$  的测试值由下图 1 给出。图中表明，在三种考虑的速率下，节点达到 100 时， $Pr_p$  保持低于  $1.6 \times 10^{-3}$  的值。



(圆：800b/s、方形：1600b/s、三角形：6400b/s)

图 1 不同数据传输率下吞吐量与终端数函数关系

仿真结果显示，当节点数从 20~40 到大约 100，数据速率从每秒几百比特到几千比特时， $(UWB)^2$  可以成功应用于无线传感器网络。

分析，同时对裁剪超宽带 MAC 协议进行了分析，通过仿真试验得出结论  $(UWB)^2$  协议可以应用于无线传感器网络。

5 结论

本文对现有无线传感器网络 MAC 协议进行了参考文献 (略)

作者联系方式

通信地址：哈尔滨市埃德蒙顿路 1 号武警黑龙江省总队通信处网管中心  
邮政编码：150070  
联系电话：0451-87120000 13115552121



# SAN over SDH在军事信息网建设中应用研究

王洋洋 廖晓闽

**摘 要：**存储区域网络（SAN）是随着光纤通道（FC）技术的出现而产生的新型存储系统，它有效地解决了信息资源的存储问题。本文通过 SDH 网络将 SAN 互连，首先比较了三种存储网络的互连方案，建立了实现 SAN 之间互连图，最后分析了 SAN over SDH 网络的恢复能力，得出 SAN over SDH 是军事信息网建设的首选。

**关键词：**SAN over SDH；信息网；互连

## 1 引言

当今社会，信息技术日新月异，信息化社会加速发展，信息总量也在迅猛地增长。有人做过这样的统计，20 世纪 60 年代社会信息总量约为 72 万亿字符，80 年代就超过了 500 万亿字符，而 1995 年的信息总量比 1985 年增长了 2400 倍，而且这种增长仍处于高速发展中。信息量的超速发展，给传统的信息存储、整合、选取和保护带来了极大的困难。在现代信息化战争的情况下，要保证军事设施在遭受严重的军事打击或者自然灾害破坏后，在很短的时间内得到迅速、高效的恢复，就需要构建一个“强健”的存储网络，以确保信息的完整性和实时性，而 SAN（Storage Area Network）就是最佳选择。SAN（存储区域网络）具有存储容量大、I/O 带宽宽、易于集中的管理和更好的数据保护、一致性好、易于灾难恢复、扩展性好、投资成本少、对全局数据的全局访问和广域性的服务能力等优点，所以一旦建立许多 SAN 后，把各个“独立”的 SAN 网络互连起来就可以实现数据的广泛和海量存储，并且其灾难恢复也将会更加容易和有效。

## 2 SAN over SDH

存储区域网络是随着光纤通道（FC）技术的出现而产生的新型存储系统。它通过不同的连接设备（如光纤集线器、光纤路由器、光纤交换机等）构成光纤通道网络，将各种存储设备（磁盘阵列、NAS（网络附属存储）、磁带等）以及服务器连接起来，形成高速专用存储子网，数据通过存储区域

网络在服务器和存储设备之间进行高速传输。所谓光纤通道是一种在系统间进行高速数据传输的技术标准，提供高性能的传输和高带宽的可视化计算，适用于 CPU、海量存储器互连的分布式计算机系统，提供类似 I/O 的带宽和并行处理能力。FC 由于其实际协议的低消耗，其实际可用带宽几乎接近于实际数据传输带宽，并且具有扩展带宽的能力，已成为 SAN 的事实标准，其协议结构见参考文献 [5]。

### 2.1 SAN互连方案比较

SAN 的建立并不难，关键就是所有 SAN 之间的互连。所谓 SAN 互连就是通过光纤信道或其他的技术实现存储设备、存储子系统与服务器组件的连通性。互连的设备有适配器、扩展器、集线器、路由器等。SAN 可以通过 WDM、IP、SDH 实现互连，下表是它们之间性能的比较。

表 1 性能比较

	SAN over WDM	SAN over IP	SAN over SDH
成本	高	低	低
业务有效性	低	高	高
服务质量	高	低	高
容量	非常高	低	高
同步/异步	同步和异步	异步	同步和异步
流控制	不好	好	好
接口类型	FC、ESCON、FICON	FC	FC、ESCON、FICON

通过表 1 中 SAN over WDM、SAN over IP 和 SAN over SDH 三种存储网络互连方案的性能比较，可以得出这三种存储网络互连方案中最优的是 SAN over SDH。

2.2 SAN over SDH方案的实现

以中心 SAN 为中心，向外成辐射状，然后再以下一级 SAN 为中心向外辐射，直到最后一级。如此一级连着一级，最终使得所有 SAN 实现互连。图 1 是实现 SAN 之间互连的简略图。

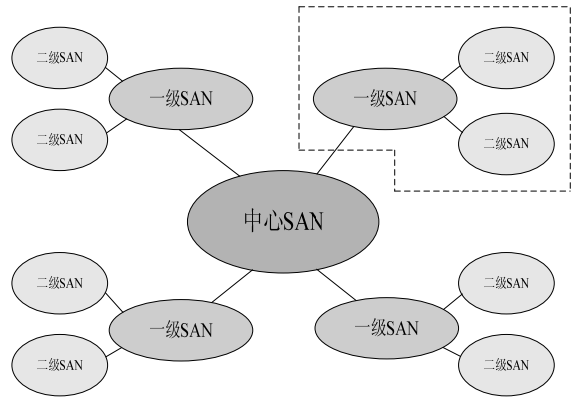


图 1 SAN 之间互连图

图 1 给出了 SAN 之间的互连，其中上级 SAN 与下级 SAN 之间的互连是通过 SDH 网络。图中中心 SAN 还可以通过 SDH 网络与更上一级的 SAN 网络互连，二级 SAN 也同样可以与更下一级的 SAN 网络互连。图 2 是图 1 中虚框的详细图示。

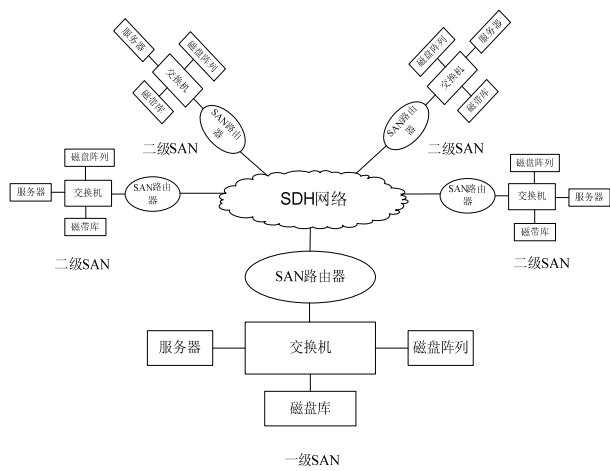


图 2 SAN over SDH 详细图

从图 2 中可以看到，各个二级 SAN 通过 SAN 路由器与 SDH 网络连接起来，SDH 网络又通过

参考文献（略）

作者联系方式

通信地址：西安市王曲镇西安通信学院九队  
邮政编码：710068  
联系电话：15929907307

SAN 路由器与一级 SAN 连接起来。这就实现了一级 SAN 与二级 SAN 的互连。如果二级 SAN 下还有三级 SAN、四级 SAN，也可以用同样的方式实现上级 SAN 与下级 SAN 的互连。当然一级 SAN 与中心 SAN 之间也是如此。如此一级连着一级，最终可以把所有的 SAN 网络都连接起来，统一到一个中心 SAN 网络上。这就使得数据不单单是在一个独立的 SAN 中存储，而是在一个全局性的 SAN 网络中存储。如果下级 SAN 网络受到破坏，其上级网络可以通过 SDH 网络对其实施快速高效的数据恢复。同样也适应与下级 SAN 对其上级 SAN 的数据恢复。

目前我军的通信网络以 SDH 为主，这就为 SAN over SDH 在我军的信息网建设中的应用提供了有力的基础。SAN 网络提供同步数据复制和快速数据恢复功能，即同样的数据被写到本地 SAN 网络（上级 SAN 网络）磁盘的同时，也被写到了远程 SAN 网络（下级 SAN 网络）磁盘，这个过程称为磁盘镜像。所以，一旦战争打起或者受严重的自然灾害的影响，某个局部 SAN 网络受到破坏，其上级或下级 SAN 网络可以通过 SDH 网络中高速的光纤通道对其数据实施迅速、高效的恢复，以确保数据的有效性。同时 SAN over SDH 存储网络还具有非常灵活的扩容方式和更安全的集中管理，故此在该网络中“添加”或“删除”是非常方便的。

3 结论

由上分析可知，SAN over SDH 是建立我军信息网的首选方案，它不但能够实现更优良的性能，更灵活的扩容以及更安全的集中管理，而且建设、维护和恢复的成本较少，很适合我国目前的国情。但是要建立一个高速、可靠、生存力强大的 SAN over SDH 网络，仍然需要我们不懈的努力，困难仍然不小。像 SAN over SDH 网络的拓扑问题、数据存储恢复策略和网络的扩容和自适应等问题，仍然需要进一步的研究。

# 基于AHP和灰色理论的战术通信网系统效能评估方法

韦涛 田永春

**摘 要:** 系统效能评估是系统研究、设计以及验证的重要手段,用来度量系统在给定的条件下满足特定要求的能力。系统效能评估涉及到系统的各个方面,不同的系统与不同的阶段采用的评估方法也不同。本文针对战术通信网的设计与建设提出了一种基于层次分析法(AHP)和灰色理论的系统效能评估方法,试图提供一种更加全面与客观的方法来衡量系统效能。

**关键词:** 系统效能; 层次分析法(AHP); 灰色理论; 战术通信网络

## 1 引言

系统效能是预期一个系统能满足一组特定任务要求程度的度量,是系统的有效性、可信性以及能力的函数,是在规定的条件下达到规定的使用目标的能力<sup>[1]</sup>。系统效能评估方法就是通过一些必要的技术性能指标,使用科学的建模与先进的分析手段与方法,衡量系统的综合能力,度量系统在给定条件下的效能,是系统研究、设计以及验证的重要手段。

系统完成特定使命的能力是通过系统的一系列功能来实现的,而这一系列的功能是通过大量的性能、指标来保证的,这些功能、性能、指标按一定的层次结构与关联关系有机汇集,就构成了系统完成特定使命任务的评估方法。即系统效能评估主要涉及两个方面的内容:评估指标体系和评估算法,评估指标体系是来源于系统的第一手资料,是系统评估的主要依据;评估算法是对系统指标进行处理,得出系统效能的计算方法。不同的指标体系对应不同的评估方法。一般用一、两个指标难以完整地、全面地评价系统的综合效能,因此必须首先确立一套相对完整的多目标多层次效能评估指标体系,在对这些主要效能指标逐一分析、评估的基础上,建立科学客观的关系模型,才能最终完成系统效能的评估。指标体系要满足一致性、可测性、完备性、独立性、客观性等要求<sup>[2]</sup>。

目前,系统效能评估的主要方法有类比法、试验法、数学模型法等,其中数学模型法包括指数法、模糊评价法、灰色决策评价方法、Petri网分析法、神经网络分析法、信息量分析法等。这些方法各有不同的适用范围与适用阶段,类比法比较适合

于方案论证阶段,用于进行横向的设计指标对比;试验法需要具有原型系统,一般用于系统建设后期与验收阶段,数学模型法一般用于系统设计与建设过程中,通常与仿真系统一起建设。

战术通信网络与固定网络或民用无线网络都不同,需要满足多种特殊的战术通信需求,不同的需求要求系统具有不同的能力。每个能力一般又可以划分为几个子能力,而每个子能力又涉及很多因素,能力之间可能也是相关的。因此表征能力的指标之间的关联度复杂,而且对于系统本身的认识程度是有限的,在评价指标体系的选取与测量时也只能获得非完全信息,指标之间无法满足独立性的要求,因此目前的数学模型法都存在评估不全面或不客观的缺点。

层次分析法(AHP)是一种定性和定量分析相结合的多目标决策分析方法,特别适合将决策者的经验判断给予量化,对目标结构复杂且缺乏必要的数据的情况。灰色理论作为研究“外延明确,内涵模糊”的理论,已经在许多方面得到广泛的应用。根据战术通信网络效能的分层结构与指标信息的非完全性和非独立性的特点,本文提出基于AHP和灰色理论的系统效能评估方法。

## 2 评估指标体系

### 2.1 评估指标的选取原则

评估指标体系是为反映评价目标的各个要素之间关系及其重要程度而建立的量化系统。它是联系主体与客体的桥梁,一方面要反映评价客体的本质属性,另一方面又要体现主体对评价对象的需要或

要求。建立一套能比较全面、客观的反映系统实际情况的评价指标体系，是建设评估系统的第一步。评估指标体系的设计遵循如下原则。

- 1) 全面性，即评估指标体系能够全面反映系统的综合实际情况，不能有任何遗漏；
- 2) 简明、适度，即有一定的科学性，大小也适宜。指标体系过大，指标层次过多，指标过细，势必将评价者的注意力吸引到细小的问题上；而指标体系过小，指标层次过少，指标过粗，又不能充分反映系统的实际水平；
- 3) 独立性，即各评价指标和相应标准相互独立；
- 4) 稳定可比性，即评价指标和标准有明确的内涵，易于在不同系统之间相比较；
- 5) 灵活可操作性，即评价指标体系具有足够的灵活性，以供决策者根据可能发生变化的实际情况，对子指标灵活运用。

2.2 评估指标的选取方法

对于系统的评估来说，通常需要同时兼顾多个

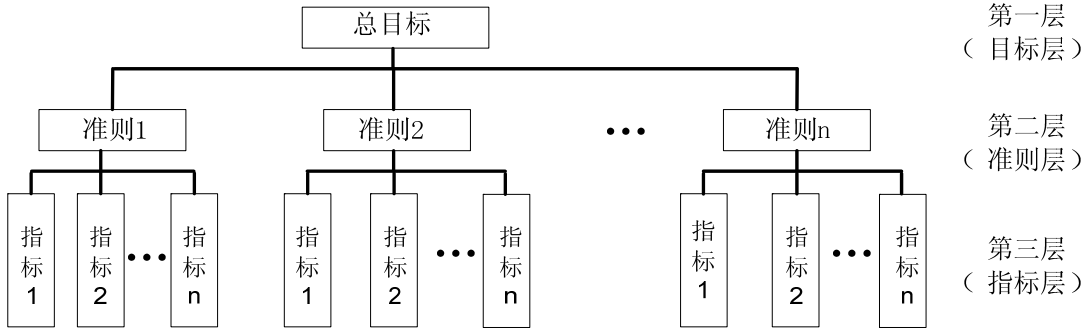


图1 评估指标体系

2.3 定性指标的量化处理

如果指标是有量化值的，则直接以数值的方式定义该指标值。但并不是所有的指标都可以是定量描述，有的指标不能进行或暂时不能给出定量的结果，而是以定性或描述性的语言给出的，如一般、强、中、弱等。这些定性指标就不能直接进行计算，必须给出定量的结果。而且某些指标可能是具有关联性的，它们对不同的上级因素可能有不同的影响因子。从灰色理论的角度考虑，这些指标都属于灰数，因此这里可以借用灰色理论，对这些灰数（即定性）进行白化<sup>[4]</sup>。

对某一定性评价指标，假设有 S 个评价者，便

目标。例如，对通信系统来说，需要通信系统的安全性高、可用性强、造价低等，这些都是评估通信系统的第一层目标。而上述的每个目标又包含不同的下层目标，例如，安全性又包括防入侵能力、保密能力等。鉴于系统的这种特征，可以借助层次分析法（AHP）<sup>[3]</sup>对系统的指标进行自顶向下层层分解的方法，根据不同的目标来划分、选择、归类。按照自顶向下的原则，评估指标的选取方法如下。

- 1) 首先根据确定评估的总目标，确定下面的准则层，也就是影响总目标的一级因素。一般每一层中，处于对等低位因素要不大于 9 个；
- 2) 再确定影响一级目标的次级因素；
- 3) 采用 AHP 法，逐级分解，逐个确定每一目标的影响因素与衡量指标。

需要说明的是，在进行指标分解时，应确保下一层次因素或指标的完备性，指标之间的关联由本文后面的方法处理。评估指标的分层选取方法如图 1 所示。

可以得到 S 个区间估计值，即： $[X_{1min}, X_{1max}], [X_{2min}, X_{2max}], \dots, [X_{smin}, X_{smax}]$ ，然后进行如下计算：

$$X_{min} = \frac{1}{S} \sum_{n=1}^S X_{nmin}$$
$$X_{max} = \frac{1}{S} \sum_{n=1}^S X_{nmax}$$

通过上两式得到灰数  $\otimes$  的灰色区间  $[X_{min}, X_{max}]$ ，即  $\otimes \in [X_{min}, X_{max}]$ ，然后根据灰数  $\otimes$  的分布信息进行白化。由于灰数  $\otimes$  在灰色区间中取值的分布信息缺乏，本文采用等权均值白化得到白化值  $\tilde{\otimes}$ ，完成对指标体系中的定性指标的

量化。如下式:

$$\tilde{\otimes} = \frac{1}{2}(X_{\min} + X_{\max}) \quad (1)$$

### 3 评估算法

获得系统的评估指标只是获得了系统的一些基本参数, 这些指标都是孤立的, 必须建立指标之间的关联关系模型, 确定每个指标对所评估的能力(评估对象)的影响程度以及作用方式, 才能客观科学地反映系统的综合效能。评估算法就是对评估指标进行有机融合的方法, 反映的是系统内部能力与性能指标之间的作用关系。

设有  $n$  个对象,  $m$  个评估指标,  $s$  个不同的灰类, 对象  $i$  关于指标  $j$  的观测值为  $x_{ij}$ ,  $i=1, 2, \dots, n$ ;  $j=1, 2, \dots, m$ , 评估算法就是要根据  $x_{ij}$  的值对相应的对象  $i$  进行评估、诊断。本文采用基于三角白化权函数的灰色评估方法, 具体步骤如下。

第一步: 按照评估要求所划分的灰类数  $s$ , 将各个指标的取值范围也相应地划分为  $s$  个类型, 例如将  $j$  指标的取值范围  $[a_1, a_{s+1}]$  划分为  $s$  个区间

$$[a_1, a_2], \dots, [a_{k-1}, a_k], \dots, [a_{s-1}, a_s], [a_s, a_{s+1}]$$

其中,  $a_k$  ( $k=1, 2, \dots, s+1$ ) 的值一般可根据实际情况的要求或定性研究结果确定。

第二步: 令  $\lambda_k = (a_k + a_{k+1})/2$  属于第  $k$  个灰类的白化权函数值为 1, 连接  $(\lambda_k, 1)$  与第  $k-1$  个灰类的起点  $a_{k-1}$  和第  $k+1$  个灰类的终点  $a_{k+2}$  得到  $j$  指标关于  $k$  灰类的三角白化权函数  $f_j^k(\bullet)$ ,  $j=1, 2, \dots, m$ ;  $k=1, 2, \dots, s$ 。对于  $f_j^1(\bullet)$  和  $f_j^s(\bullet)$ , 可分别将  $j$  指标取值域向左、右延拓至  $a_0, a_{s+2}$  (如图 2)。

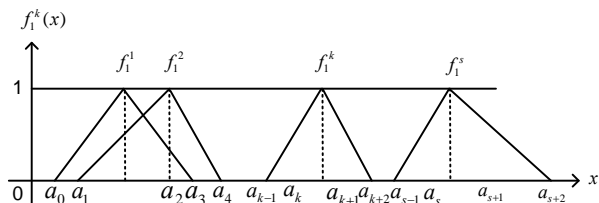


图2 计算方法

对于指标  $j$  的一个观测值  $x$ , 可由公式

$$f_j^k(x) = \begin{cases} 0, & x \notin [a_{k-1}, a_{k+2}] \\ \frac{x - a_{k-1}}{\lambda_k - a_{k+1}}, & x \in [a_{k-1}, \lambda_k] \\ \frac{a_{k+2} - x}{a_{k+2} - \lambda_k}, & x \in [\lambda_k, a_{k+2}] \end{cases} \quad (2)$$

计算出其属于灰类  $k$  ( $k=1, 2, \dots, s$ ) 的隶属度  $f_j^k(x)$ 。

第三步: 计算对象  $i$  ( $i=1, 2, \dots, n$ ) 关于灰类  $k$  ( $k=1, 2, \dots, s$ ) 的综合聚类系数  $\sigma_i^k$ :

$$\sigma_i^k = \sum_{j=1}^m f_j^k(x_{ij}) \cdot \eta_j \quad (3)$$

其中,  $f_j^k(x_{ij})$  为  $j$  指标  $k$  子类白化权函数;  $\eta_j$  为指标  $j$  在综合聚类中的权重, 并且  $\sum_{j=1}^s \eta_j = 1$ 。综合聚类系数  $\sigma_i^k$  的含义就是对象  $i$  属于该灰类的程度。由于有  $s$  个灰类, 因此这里也就有  $s$  个综合聚类系数;

第四步: 由  $\max_{1 \leq k \leq s} \{\sigma_i^k\} = \sigma_i^{k^*}$ , 判断对象  $i$  属于

灰类  $k^*$ , 即在  $s$  个综合聚类系数中取出最大值, 并确定对象  $i$  在  $j$  指标下属于该灰类  $k^*$ ; 当某个对象在不同的指标下同属于  $k^*$  灰类时, 还可以进一步根据综合聚类系数的大小确定该对象处于不同指标下的优劣或位次。

第五步: 确定系统效能。假设系统效能有  $m$  个评估指标(准则),  $s$  个不同的灰类, 对象  $i$  关于指标  $j$  的观测值为  $x_j$ ,  $j=1, 2, \dots, m$ , 因此也可以通过第一步到第四步来确定某一准则在某指标组下的评估值(最大综合聚类系数)。在最终确定系统效能时, 准则层就成为指标, 首先根据 2.3 节确定某一准则的指标值, 在量化过程中要考虑该准则在下一级指标作用下的综合聚类系数。因此可以重复第一步到第四步来求得系统效能的综合聚类系数, 在第三步计算时, 需要将准则在下一级指标作用下的综合聚类系数考虑进去, 即作为其对整体效能的贡献, 因而, 在计算系统效能关于灰类  $k$  ( $k=1, 2, \dots, s$ ) 的综合聚类系数  $\sigma^k$ , 需用下式:

$$\sigma^k = \sum_{j=1}^m f_j^k(x_j) \cdot \sigma^o \cdot \eta_j \quad (4)$$

上式中 $\sigma^\circ$ 为准则在下一级指标作用下的综合聚类系数。

评估算法的目的是建立指标与评估对象之间的关联关系模型，通过该模型，在输入评估指标参数后，就可以获得评估对象（评估能力）的定性值，该值反映了系统在该方面能力的高低。这样逐层计算，可以最终获得系统效能的客观度量。系统的综合效能可用来对不同的系统进行分析对比，对方案进行择优，而对不同能力的评估可用来分析系统设计与建设过程中方案缺点与改进途径。

本文评估算法的主要优势在于，它不仅具有系统的整体效能评估能力，而且也具有系统某一方面

的评估能力。在计算系统整体效能时，充分考虑系统某一方面对系统整体效能的作用，通过综合聚类系数将两者关联起来，体现了系统某一方面对整体效能的贡献，评估更加客观科学。

4 计算示例

下面以战术通信网的效能评估为例来介绍本文算法的使用方法。图 3 为对应于图 1 的战术通信网效能层次划分的简单示意图，实际情况还要根据性能指标进行全面细致的分层。

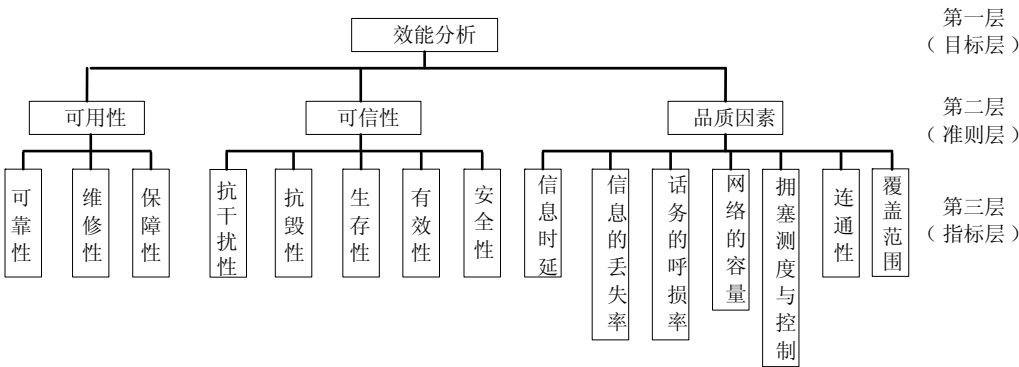


图 3 战术通信网评估方法

下面使用上述评估方法，来评估战术通信网的总体效能。

第一步：定性指标量化。

对定性描述的指标进行量化，例如上图中指标层中的安全性是一个定性指标，只能以语言进行描述，例如安全性高、中、低，我们采用 100 制，根据 S 个评价者给出的评价区间，采用 2.3 的计算，得出定性指标的白化值。

第二步：确定准则层和目标层的评判矩阵。

图 3 中准则层分别有可用性、可信性、品质因素三个，可以根据要求给出每一准则的评判矩阵。目标层的总体效能只有一个，也可以给出它的评判矩阵。例如假设图 3 中的抗毁性可分为连通度、粘聚度、分散度，那么可以建立抗毁性指标的评判矩阵，并且抗毁性的量化指标由其下层的指标计算出。

下面以可用性为例说明评估计算过程。

设可用性的评判矩阵为：{高、中、差}，其他准则的评判矩阵这里不再详述。战术通信网总体效能的评判矩阵为：{优、良、中、及格、差}。

第三步：可用性的评估计算。

设可用性关于下层指标的值为 $x_1, x_2, x_3$ ，这里的可用性对应第 3 章中的评估对象 i，可靠性、维修性、保障性对应第 3 章中的指标 j， $x_1, x_2, x_3$ 分别为指标的观测值，因此可以得到指标关于对象的观测值矩阵为： $[x_1, x_2, x_3]$ 。因此计算步骤如下。

(1) 将指标划分区间

由于可用性的评判矩阵为：{高、中、差}，所以相当于将其划分为三个灰类。然后根据第 3 章中评估算法的第一步将可靠性、维修性、保障性分别划分为三个类型，即分别将可靠性、维修性、保障性都划分为三个区间。

(2) 得出各指标的白化权函数

根据第 3 章中评估算法的第二步，分别得出可靠性、维修性、保障性三个指标的白化权函数 $f_j^k(x)$ ， $j=1, 2, 3, k=1, 2, 3$ ，这里 j 分别代表指标的可靠性、维修性、保障性，k 代表灰类，对应评判矩阵中的 {高、中、差}。

(3) 计算综合聚类系数

根据第 3 章中评估算法的第三步，可由式 (3-2) 计算可用性的综合聚类系数，即：

$$\sigma_i^k = \sum_{j=1}^3 f_j^k(x_{ij}) \bullet \eta_j$$

这里  $i$  表示评估对象代号,  $f_j^k(x_{ij})$  表示可靠性、维修性、保障性三个指标分别在自己白化权函数中的取值,  $\eta_j$  为指标  $j$  在综合聚类中的权重, 即可靠性、维修性、保障性三个指标在综合聚类中的权重, 可通过研究与评估的侧重来综合选取。

#### (4) 确定可用性处于的灰类

确定可用性处于的灰类, 也就是确定可用性处于评判矩阵中的哪个档次, 根据第3章中评估算法的第四步可以得出。

#### 第四步: 确定战术通信网的总体效能

利用第三步类似的方法可以求得可信性和品质因素所属的灰类, 再根据所属灰类和式(2-1), 对可用性、可信性、品质因素指标进行量化。然后按照战术通信网的总体效能的灰类数, 即评判矩阵: {优、良、中、及格、差}, 将可用性、可信性、品质因素划分相应多个灰类, 也就是五个灰类。根据式(3-3)得出战术通信网总体效能的综合聚类

系数:

$$\sigma_i^k = \sum_{j=1}^3 f_j^k(x_{ij}) \bullet \sigma_j^k \bullet \eta_j$$

这里  $\sigma_j^k$  表示下层指标的综合聚类系数, 这里分别表示可用性、可信性、品质因素的综合聚类系数。

最后, 确定战术通信网总体效能的所属的灰类, 即评判系统效能的优劣。

## 5 总结

本文以战术通信网为研究目标, 提出了一种结合层次分析法和灰色系统理论的系统效能评估方法, 充分考虑战术通信网络指标之间的关联性与复杂性, 使评估的结果更加合理可信。评估方法不仅可以对不同系统效能进行比较, 也可以对某一子能力进行比较, 具有较好的灵活性与扩展性。

## 参考文献 (略)

## 作者联系方式

通信地址: 成都 810 信箱 15 分箱中国电子科技集团公司第三十研究所

邮政编码: 610041

联系电话: 028-85169049

# 虚拟化存储技术研究

翁伟兵 吴建国 康东明

**摘 要:** 数据存储容量不断增长, 业务连续性需求日益迫切, 以 SAN 为代表的各种存储技术方兴未艾, 这对存储系统的使用、管理和维护提出了一个更高的要求, 虚拟化存储技术提供了相应的功能, 本文阐述了虚拟化存储技术的原理和机制, 介绍了虚拟化存储技术的主要功能特点, 提出了基于虚拟化存储技术的数据保护初步设想。

**关键词:** 存储; 网络; 虚拟化; 数据保护

## 1 虚拟化存储的提出

随着计算机技术和数据存储技术的进一步发展, 存储系统在 IT 系统的地位也越来越重要。同时, 存储系统也面临着越来越复杂的管理问题, 主要表现为: 首先是数据的爆炸式增长使得对存储设备的管理成本远远高于硬件采购成本, 其次对数据存储需求的不可知导致存储设备的平均利用率不高, 第三, 在需要扩容时, 原有设备和新增设备的产品类型不同, 无法进行统一管理, 第四, 由于计划内或计划外的存储配置的变更, 必然导致应用系统停机, 无法实现对业务的可持续性要求。

在这种使用背景下, 虚拟化存储技术适时地出现在用户面前。对于虚拟化的解释, SNIA (国际存储网络工业协会) 的存储网络术语字典是这样表述的。

虚拟化——通过将一个(或多个)目标(Target)服务或功能与其他附加的功能集成, 统一提供有用的全面功能服务。典型的虚拟化包括如下一些情况: 屏蔽系统的复杂性, 增加或集成新的功能, 仿真、整合或分解现有的服务功能等。虚拟化是作用在一个或者多个实体上的, 而这些实体则是用来提供存储资源或/及服务的。

这是一个抽象的概念, 我们可以理解为: 虚拟化存储提供了一种能力, 它能把异构的主机服务器连接到分布式的异构存储设备池中, 并且可以动态地、透明地将存储资源分配到各种应用系统, 满足不同应用系统对存储的变化需求。虚拟存储技术将底层存储设备进行抽象化统一管理, 向服务器层屏蔽存储设备硬件的特殊性, 而只保留其统一的逻辑特性, 从而实现了存储系统集中、统一而又方便的

管理。

## 2 虚拟化存储的类型

虚拟化是一个处理过程, 这个处理过程一定是在主机和存储设备之间完成的。根据数据读取的流向, 虚拟化过程可能在三个位置完成: 主机、存储设备和存储网络。事实上, 在三个位置上都有相应的虚拟存储技术存在, 根据虚拟化处理所在的位置, 虚拟存储技术被分为“基于主机端的虚拟存储”、“基于存储设备的虚拟存储”以及“基于存储网络的虚拟存储”这三种类型, 如图 1 所示。

### 2.1 基于主机的虚拟化存储

基于主机端的虚拟化存储主要应用于单个服务器需要访问多个物理磁盘的使用方式, 几乎都是通过纯软件的方式实现的, 这种实现机制不需要引入新设备, 也不影响现有存储系统的基本架构, 所以实现成本较低。通常由主机操作系统下的逻辑卷管理软件(logical volume manager)来实现, 逻辑卷管理器既可能是操作系统的一部分, 也可能是某个独立的软件, 它在主机上建立一个虚拟层, 通过这个虚拟层, 物理磁盘或者 LUN 被组织成逻辑磁盘组和逻辑卷, 基于主机的虚拟化存储方式如图 2 所示。

基于主机进行虚拟化的最大优点是其久经考验的稳定性以及对异构存储系统的开放性。它与文件系统共同存在于主机上, 便于二者的紧密结合以实现有效的存储容量管理。但是其难以克服的困难是由于缺乏最终的控制机能, 对平台依赖性太强, 而且由于虚拟管理的复杂计算必然要占用大量服务器



主机和内存资源，因此这种方式在一定程度上影响服务器应用系统的运行效率。

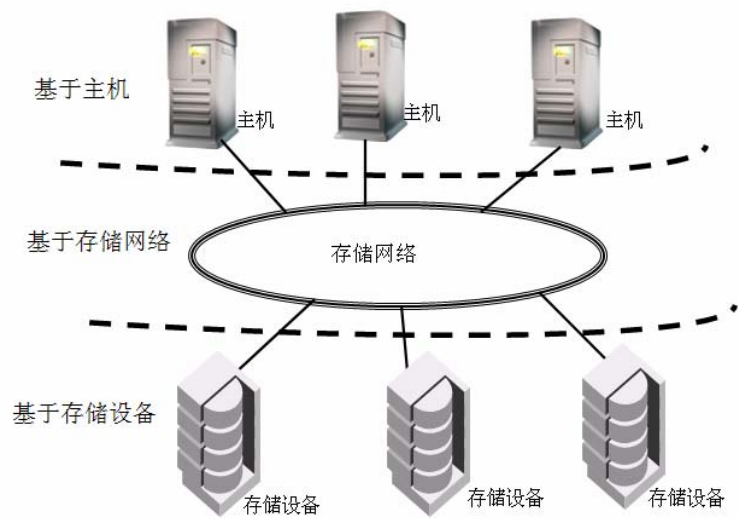


图 1 虚拟化存储类型

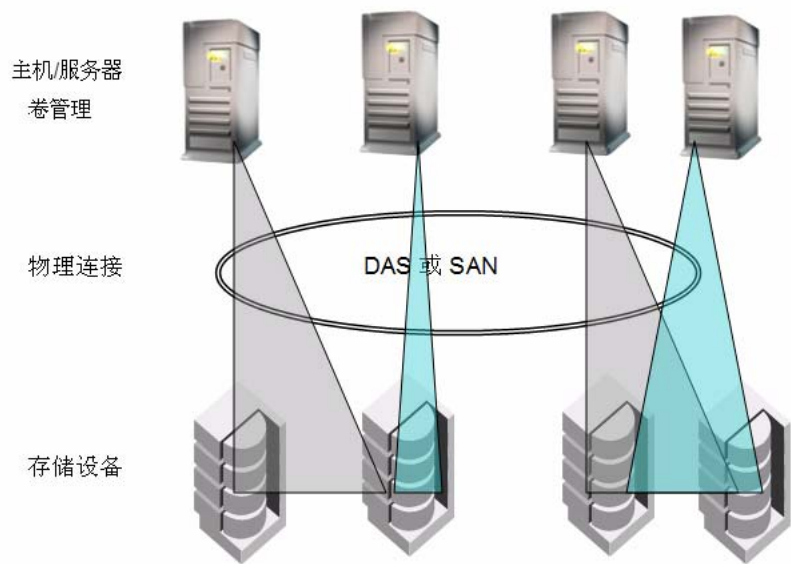


图 2 基于主机的虚拟化存储

## 2.2 基于存储设备的虚拟化存储

基于存储设备的虚拟化存储主要应用于多个服务器需要访问同一个磁盘阵列的使用方式，此时虚拟化的工作是在阵列控制器上完成，将一个阵列上的存储容量划分多个存储空间（LUN），供不同的主机系统访问。智能的阵列控制器提供数据块级别的整合，同时还提供一些附加的功能，例如：LUN 映射、缓存、快照、数据复制等。配合使用不同的存储系统，这种基于存储设备的虚拟化模式可以实

现性能的优化，基于存储设备的虚拟化存储方式如图 3 所示。

这种基于存储设备的虚拟化不依赖于某个特定主机，能够支持异构的主机系统，但是对于每个存储子系统而言，它又是一个专用私有的方案，不能够跨越各个存储设备间的限制，无法打破设备间的不兼容性。因此使用基于存储设备虚拟化技术虽然有效率高、性能好等特点，但是在实际应用中，几乎所有的厂商都只提供对自身产品的支持，其开放性和多类型存储系统的兼容性就大打折扣。

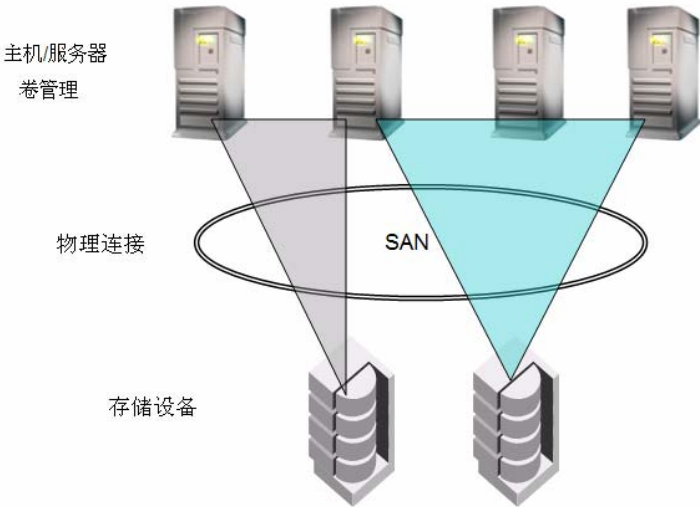


图3 基于存储设备的虚拟化存储

2.3 基于存储网络的虚拟化存储

以上两种方式都是一对多的访问模式，而在现实的应用环境中，很多情况下是需要多对多的访问模式的，也就是说，多个主机服务器需要访问多个异构存储设备，目的是为了优化资源利用率----多个用户使用相同的资源，或者多个资源对多个进程提供服务，等等。在这种情形下，存储虚拟化的工作就一定要在存储网络上完成了。

基于存储网络的虚拟化存储主要应用于多个服

务器需要访问多个异构存储资源的使用方式，这是一种实际应用中最普遍也是最复杂的虚拟存储技术。它将不同的存储设备整合到一个 SAN 中统一为各种不同的应用主机提供容量，它包括两个层面，一是将不同的存储资源进行统一整合，形成一个大的存储池，；二是对存储池容量的再分配，可以根据应用主机的需求任意切分容量，可以最大限度地增加存储资源的利用率，基于存储网络的虚拟化如图 4 所示。

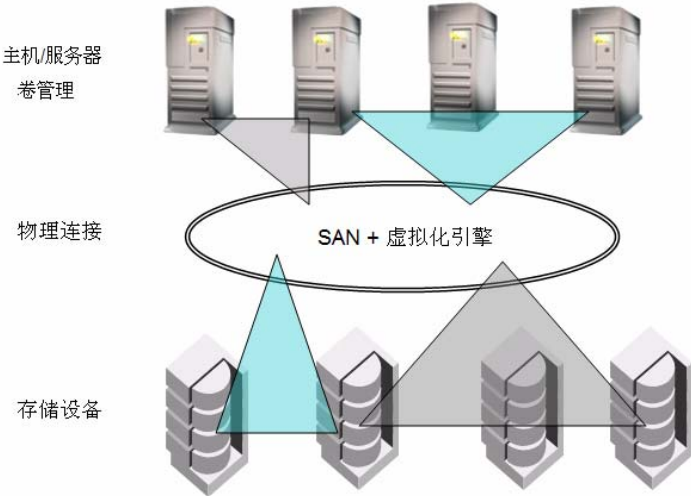


图4 基于存储网络的虚拟化存储

在存储网络层面进行虚拟化的方法已经成为存储虚拟化的明确方向，这种虚拟化工作需要使用相应的专用虚拟化引擎来实现。所谓的虚拟化引擎，是一种专用的存储管理服务器，用它来完成上面的

两方面虚拟化工作，即将多个物理磁盘系统组合成大的存储空间或者把它们分割成小的存储单元，并根据主机对容量、速度和可用性的要求，将这些存储单元分配给主机使用。

这种用作虚拟化引擎的专用存储服务器，或是建立在某种专用的平台上，或是在标准的 Windows, Unix 和 Linux 服务器上配合相应的虚拟化软件而构成。在这种模式下，因为所有的数据访问操作都与虚拟化引擎相关，所以必须避免它的单点故障，因此在实际应用当中，虚拟化引擎通常都是冗余配置的，以保证它的高可用性（HA）。

### 3 虚拟化存储的实现方式

虚拟化引擎可以用两种方式来控制存储的虚拟化：直接位于主机服务器和存储设备的数据通道中间——带内方式（In-Band）；或者是位于数据通道之外，仅仅向主机服务器传送一些控制信息——带外方式（Out-of-Band）。“带内”和“带外”，区别就在于数据流是否必须通过虚拟化存储引擎传输。带内方式则需要改变信息的路径，所有信息（控制流及数据流）都要通过虚拟化存储引擎传输并进行处理，实现对存储空间全面控制，一般带外虚拟化存储引擎不改变数据流的传输方式，只接收信息的控制流，完成物理设备和逻辑卷之间的地址映射而已。

#### 3.1 带内虚拟化存储

带内虚拟化引擎位于主机和存储系统的数据通道中间，控制信息和用户数据都会通过它，而它会将逻辑卷分配给主机，就像一个标准的存储子系统一样。因为所有的数据访问都会通过这个引擎，它就可以实现很高的安全性。就像一个存储系统的防火墙，只有它允许的访问才能够通行，否则就会被拒绝。这种方式的虚拟化，不需要在主机上安装特别的虚拟化驱动程序，比带外方式易于实施，并且支持广泛的异构存储系统，具有很好的互连性。

#### 3.2 带外虚拟化存储

带外虚拟化引擎物理上不位于主机和存储系统的数据通道中间，而是通过其他的网络连接方式与主机系统通讯。于是，在每个主机服务器上，都需要安装客户端软件，或者特殊的主机适配卡驱动，这些客户端软件接收从虚拟化引擎传来的逻辑卷结构和属性信息，以及逻辑卷和物理块之间的映射信息，在 SAN 上实现地址寻址。存储的配置和控制

信息由虚拟化引擎负责提供。这种方式的实施难度大于带内模式，因为每个主机都必须有一个客户端程序。

## 4 虚拟化存储的主要功能

本文所讨论的虚拟化存储技术的主要功能主要是针对基于存储网络的带内虚拟化存储技术，实现方式可以是内置式，即把虚拟化引擎内嵌到光纤交换机设备中，也可以是外挂式，即虚拟化引擎安装在特定的硬件设备上，再连接到光纤存储网络中。

### 4.1 集中管理功能

虚拟化存储能将不同厂商的不同类型的存储设备连接在一起进行集中管理，将多个不同的存储资源整合到统一的存储池中，它包括两个方面的整合，一是不同厂商的存储设备的整合（如 EMC、HDS、HP、IBM 等），二是不同接口协议的存储设备的整合（如 SCSI、iSCSI、Fibre Channel 或 Infiniband 等）。在现有存储设备中，同厂商设备原则上都能支持多台设备的整合，但不同厂商的设备由于技术体制方面的制约很难整合在一起；另外，不同接口协议的存储设备在设备自身的管理平台上还不能整合在一起。虚拟化存储管理技术提供了这个能力。

### 4.2 存储资源虚拟化

基于存储网络的虚拟化存储架构管理方式能将存储资源虚拟化，并将这些虚拟存储资源整合到一个统一的存储池中，服务器主机的容量再由虚拟化引擎从这个存储池中分配。从数据流向来看，主机访问所属的存储设备时中间经过了虚拟化存储管理设备。服务器主机针对的是一个虚拟的存储设备，而不再是一个实际的物理存储设备，主机并不知道自己的存储容量物理位置在哪，借助这个存储池，服务器对虚拟存储设备的访问就如同逻辑上的本地连接设备一样，可以随时进行存储操作和管理。

### 4.3 按需提供容量

主机面对的是虚拟化引擎，它是从虚拟的存储池中获得容量的，虚拟化引擎面对的是不同的物理

存储资源，由这些物理存储资源整合成一个大的存储池。这就给主机对于存储容量的使用提供了方便，即主机能够根据应用需求在线从存储池中扩充容量，这个动作完全由虚拟化引擎来完成，避免了应用系统因存储容量扩充必须停机而带来的不便，在一定的程度上保护了用户的投资，作到了按需提供容量；同时虚拟化引擎管理的存储池也能通过增加物理存储设备而使这个存储池容量增加，基于虚拟化技术，增加的物理存储资源与已有的物理存储资源没有必然的关联。

#### 4.4 存储高级服务

基于虚拟化引擎可以提供数据存储的高级服务，主要体现在数据的复制和数据的迁移，数据复制包括同步镜像、异步镜像、异步复制等技术，这些数据复制技术本文不再赘述，但是基于虚拟化引擎的这些数据复制技术最突出的特点是它脱离了主机应用系统的干预，是在后台完成的，可以大大释放主机的应用资源，基于虚拟化平台的数据复制技术提供了数据保护的多种方式和业务连续的基本条件。

## 5 虚拟化存储的服务质量管理

在虚拟化存储管理系统中，针对不同的数据类型和数据访问性能要求，把相应的数据存放在不同存储空间中，也就是如何根据数据业务的需要，合理化利用存储空间，高效管理存储设备。如关键的、需要高速实时访问的数据存放在高端的磁盘阵列中，非关键的、低速访问需求的数据可以存放在低端的磁盘阵列或磁带系统中。通过虚拟化存储服务的质量管理可以提高存储空间的利用率，降低存储成本，同时提高数据存储服务质量。

## 6 结束语

虚拟化存储技术的提出已经有二十年的经史了，但真正涉及基于网络的虚拟化还是在 SAN 技术出现以后，近年来，随着用户数据日益增长的现实和业务连续性要求日益迫切的需求，虚拟化存储技术得到了飞速发展，但目前各厂家的技术体制不尽相同，虚拟化的标准还有待制定和完善，相信在不久的将来，虚拟化存储技术将以一种通用的、规范的技术体系为用户提供尽善尽美的数据存储服务。

### 参考文献

- [1] 网络存储技术 赵文辉等. 北京：清华大学出版社，2005
- [2] 存储区域网络精华-深入理解 SAN Richard Barker 著. 舒继武译. 北京：电子工业出版社，2004
- [3] 存储区域网络设计. Tom Clark 著. 邓劲生译. 北京：电子工业出版社
- [4] 存储区域网络精髓. 北京：电子工业出版社

### 作者联系方式

通信地址：北京市丰台区大成路 13 号 W01

邮政编码：100039

联系方式：010-66820384 13311373875

# 信息化战争条件下的雷达防护

吴爱民 万福

**摘 要:** 本文介绍在信息化战争条件下, 雷达的防护措施, 使雷达免遭反辐射导弹、巡航导弹和 GPS 制导航空炸弹的摧毁, 解除低空、超低空飞行的武装直升机、飞机和隐形飞机对雷达的威胁。介绍一种由毫米波雷达、光电成像、红外热成像组成的复合告警装置与近程密集阵火炮组成的对抗反辐射导弹、巡航导弹及 GPS 制导航空炸弹摧毁的雷达防护系统。

**关键词:** 雷达防护; 反辐射导弹; 雷达装甲

## 1 引言

“雷达是军事上的千里眼”。雷达用于探测远距离的固定和移动目标(飞机、军舰、导弹、车辆等)。雷达是一体化联合作战的最主要传感器。如在美国国家导弹防御系统(NMD)和战区导弹防御系统(TMD)中的远程相控阵雷达(地基和舰载雷达), 星载合成孔径侦察雷达, 起着预警、探测、跟踪和作战效果评估的作用。由于雷达在信息化战争中的极其重要的作用, 已成为摧毁的首选目标。在信息化战争条件下, 侦察技术高度发达、侦察装备精良(如太空侦察卫星、电子战飞机), 攻击武器非常先进(如隐形飞机、反辐射导弹等), 使雷达面临着巨大威胁。目前, 现代雷达面临着三大威胁: 隐身、干扰和反辐射导弹摧毁。在雷达反隐身技术上, 可以采用双多基地雷达组网技术, 星载雷达侦察技术和红外、热成像技术加以克服。在雷达反干扰问题上, 随着科学技术的发展, 新型的器件不断出现, 许多现代技术在雷达中的应用, 特别是计算机技术和信号处理技术在雷达中的应用, 使雷达的战术技术性能越来越强。比如相控阵雷达中采用功率和多波束控制技术、多波段伪随机自适应频率捷变技术、低截获概率技术, 使雷达抗干扰的能力大大增强, 通过战术对抗, 基本可以抗击干扰问题。目前, 雷达面临的最大威胁是来自空中机载反辐射导弹、巡航导弹和 GPS 制导的航空炸弹的致命威胁。如在海湾战争刚刚开始时, 美国空军发射了 1000 多枚反辐射导弹、巡航导弹和 GPS 制导的航空炸弹, 彻底摧毁了伊军的防空雷达系统。一般来说, 采用精确制导弹药直接摧毁雷达比采用干扰设备来削弱或破坏雷达的功能效果更佳、更容

易、更简单、更迅速、更彻底, 并且成本更低。因为, 只要雷达存在, 就总会采取各种对抗措施, 对飞机造成威胁。而对雷达的干扰对抗, 需要昂贵的对抗装备, 付出巨大的人力和花费大量的时间。干扰设备还容易暴露, 会受到打击。对雷达的防护, 是信息化战争的重要内容。能否使雷达在战争中不被摧毁或不易被摧毁、能否使雷达抗打击、迅速恢复作战性能、正常发挥战术技术性能、及时发现入侵的飞机和导弹, 是夺取战争胜利的关键。

## 2 反辐射导弹巡航导弹和GPS制导航空炸弹对雷达的威胁

### 2.1 反辐射导弹对雷达的威胁

反辐射导弹是一种利用雷达的电磁波辐射引导, 攻击敌方雷达及其载体的导弹。反辐射导弹一般以飞机为载体, 弹体内安装有雷达波束搜索、截获与制导装置。当地面雷达在搜索或跟踪飞机时, 雷达照射在飞机上的电磁波束被飞机捕获, 飞机即可发射反辐射导弹。反辐射导弹就顺着雷达的电磁波波束指向, 飞向雷达, 直至击中雷达或在接近雷达时自行引爆, 利用破片摧毁雷达和杀伤雷达操作员。如美国 1965 年装备部队的 AGM-45 “百舌鸟”导弹, 在越南战争中发挥了重要作用。现代反辐射导弹已具有记忆功能。如美国 AGM-78 “标准”导弹, 有频率记忆和位置记忆装置, 对捷变频雷达和突然停止发射电磁波的雷达, 同样能精确攻击。这样, 即使雷达在跟踪过程中发现飞机施放反辐射导弹(在雷达荧光屏上可以看到迅速接近雷达的反辐射导弹的目标亮点), 立即关机, 停止发射

电磁波，也不能排除反辐射导弹的致命攻击。AGM-88“哈姆”反辐射导弹还具有隐身功能。一般防空火控雷达难以捕捉。AGM-122A“佩剑”导弹集以上导弹的优点于一身，功能更强，射程可达25千米，速度达到3马赫。由于反辐射导弹越来越先进，已造成对雷达的致命威胁。

## 2.2 巡航导弹对雷达的威胁

巡航导弹是一种在大气层内飞行，利用气动升力支持其重量，依靠发动机的推动克服前进阻力，大部分时间近似匀速、等高状态飞行的导弹。巡航导弹有机载和舰载。在获取地面雷达的具体位置后（经度、纬度和高度），将位置参数输入导弹计算机，发射后可以不管，自动飞向目标。巡航导弹一般用复合制导装置，射程远、精度高。是一种智能型武器。美国的BGB-109C/D“战斧”导弹，采用惯性+GPS+地形匹配+景象匹配复合制导，速度0.7马赫、射程1600千米、命中精度（CEP）6米，可以从水面舰艇和潜艇发射。联合防区外空对面导弹（JASSM），采用惯性导航/GPS卫星制导+红外成像末制导，射程320千米，精度（CEP）6米，通过F-16、B-1、B-2、F117、P-3C、F-22等飞机携带，可以从防区外攻击目标。由于在导弹中安装了GPS制导装置，使巡航导弹作战精度不随射程长短而改变。GPS对导弹的制导原理是：先在导弹中装填拟攻击目标的位置参数，如高度、经度和纬度。导弹在飞行过程中，弹体中的GPS接收机不断接收GPS送来的位置信号，通过计算获得导弹自身的实时位置，将导弹的实时位置与目标位置比较，得出误差位置信息，如高度、经度和纬度误差。把误差信息通知导弹驾驶仪，驾驶仪通过设定的飞行路线修正航线，使导弹不断接近目标，直至摧毁目标。采用惯性+GPS+地形匹配+景象匹配复合制导的巡航导弹，其飞行航线还可以通过程序任意设定，使导弹进行不规则运动，如盘旋形、蛇形或半圆形运动等等。通过地形匹配，导弹可以根据地形地貌飞行，比如穿过山谷，超低空飞行，躲避防空雷达系统，规避地面炮火和导弹拦截等。采用复合制导的巡航导弹抗干扰能力极强，除非用专门的GPS接收机干扰机对飞行区域内的巡航导弹内的GPS接收机进行干扰，或对战区相应太空中的GPS发射机进行干扰，否则很难奏效。对GPS的干扰由于技术难度高，需要专门的设备，只有个别军事

大国可以做到。由于巡航导弹有发射后不管的功能、射程远、防区外可随时同时发射很多枚导弹，可以同时摧毁防空雷达网中的所有雷达，对不设防的雷达防空系统造成极其致命的威胁。

## 2.3 GPS制导航空炸弹和激光制导炸弹对雷达的威胁

GPS制导航空炸弹是一种用GPS制导、没有发动机、只靠重力滑翔飞行的炸弹。这种炸弹价格便宜，威力大，通过飞机携带。飞行中的飞机通过测距装置测算出雷达的位置后，把雷达的位置数据输入到炸弹中，释放这种航空炸弹，通过重力作用和GPS制导，炸弹滑翔飞向雷达，打击精度在（CEP）6米，是一种“长眼睛”的廉价炸弹。如GBU-87/B“石眼II”多用途集束炸弹、燃料空气炸弹等。GPS制导航空炸弹由于没有动力，难于作复杂的规避运动，体积大，速度慢，射程短。激光制导炸弹通过飞机发射激光束照射目标，炸弹顺着激光束飞向目标，其精度可以达到（CEP）3米。这种炸弹体积可以做得很大，速度慢，但威力大。如GBU-28激光钻地炸弹等。以上两种炸弹在进行攻击时，需要飞机为载体，激光炸弹还需要飞机激光照射为其指示目标，飞机载体容易受到攻击。由于这些炸弹需要飞机运载，射程短，最有效防御方法，就是通过防空系统攻击载机及通过雷达防护系统同时攻击载机和拦截航空炸弹。为了在雷达被GPS制导航空炸弹和激光制导炸弹击中时能尽量减少损失，尽快恢复战斗力，可以采取把雷达收发射机放置在坚固的地下工事内，保护收发射机，当天线被击中后，可以迅速更换，恢复雷达战斗力。把雷达操作员安排在远离收发射机的坑道中，保证雷达操作员的安全。

## 3 复合告警装置与近程密集阵火炮组成的雷达防护系统

在传统的战争中，雷达是一种进攻性武器，当雷达探测到目标后，可通知其他兵器对目标进行攻击（如飞机拦截），由于反雷达武器还没有发展到能够足以威胁雷达生存的地步，因此各国都没有对雷达的生存采取防护措施。到目前为止，世界上几乎没有对雷达进行防护的措施。这种现象使雷达的

生存日益艰难。地基雷达由于担任重要的对空对海预警任务,非常重要。由于雷达平时的战备值班,在太空侦察系统、空中电子侦察机和间谍的侦察下,其位置基本都处于暴露状态,战时很容易首先受到打击。在现代的几场战争中,雷达几乎都没有设防,都很轻易地被摧毁了。一旦雷达被摧毁,则整个防空系统就瘫痪了。“无恃其不来,恃吾有以待也;无恃其不攻,恃吾有所不可攻也。”在信息化战争条件下,需要有切实可靠的雷达防备措施。要解决雷达面临的紧迫的反辐射导弹、巡航导弹和GPS制导的航空炸弹的严重威胁问题。而反辐射导弹、巡航导弹和GPS制导的航空炸弹由于体积小、速度快、交战时间短、机动灵活、抗干扰能力强,不易用导弹进行拦截,用一般火炮拦截射击也难于奏效。这就是现代的几场战争中雷达屡屡遭受毁灭性打击的原因。

由毫米波雷达、光电、红外热成像组成的复合告警装置与近程密集阵火炮组成雷达防护系统是反辐射导弹的克星。毫米波雷达是一种基本上不受天气条件影响,可以全天工作的小功率近距离探测雷达。毫米波雷达利用目标接近雷达时径向速度产生的多普勒效应这种特征准确探测逼近的导弹,并发出告警信号。毫米波雷达对高速飞行的导弹和航空炸弹特别敏感,可以准确实时告警,灵敏度高。光电成像告警装置通过光学途径获取导弹图像并进行图像识别与特征分析,发出告警,主要是在白天进行导弹或航空炸弹逼近告警。红外热成像告警装置利用导弹尾流产生的热量进行成像并加以特征提取与分析,发出告警,可以工作在白天和夜间。三者可以组合在一起,形成一个复合告警装置,可以增强抗干扰能力,提高可靠性。复合告警装置可以有效地探测并告警高速飞行的隐形反辐射导弹、巡航导弹和由GPS制导的航空炸弹。这种雷达防护系统对任何具有以上特征的接近雷达的物体都有打击功能。比如用于打击低空、超低空飞行的飞机、隐形飞机,非常有效。因为隐形飞机对复合告警装置没有隐身功能,低空和超低空飞行的隐形飞机。即使安装有电子对抗飞机设备的电子战飞机,也难于同时对以上复合告警系统进行有效干扰。

由于雷达所需要的防御范围很小,半园半径为5000米以内。在导弹进入雷达防御区域时才进行防御性攻击,可以使告警装置全方位的告警。只要导弹接近雷达,密集阵火炮接到告警系统的信号,

控制密集阵火炮指向来袭导弹方向开火,在来袭导弹前方的特定区域形成一个拦截弹幕,摧毁来袭导弹。美国的密集阵火炮系统由6管20毫米火炮组成,弹丸初速1030米/秒,3000~45000发/分钟,最大射程1470米,仰角-25~+85度,方位310度。俄罗斯的AK-630密集阵火炮系统由6管20毫米火炮组成,4000~5000发/每分钟,最大射程4000~5000米,仰角-12~+85度,方位360度,采用H波段雷达搜索和H波段雷达+光电/光学跟踪。使用近程密集阵火炮来拦截导弹是首选的雷达反导弹战术。反应时间在4秒钟内的密集阵火炮系统可以对付0.7马赫的巡航导弹和航空炸弹。而对付3马赫飞行的高速导弹,最大射程为1470米的密集阵火炮系统与导弹的交战时间在0.1秒~1.2秒内,交战半球半径在50米~1500米。

利用这种雷达防护系统,基本上可以消除反辐射导弹、巡航导弹和GPS制导的航空炸弹对雷达的威胁。同时,可以大大提高敌方对雷达进行电子对抗的成本,大大提高地方摧毁雷达的成本和难度。因为,电子战飞机在战场区域进行作业时,随时都面临反辐射导弹和其他兵器的致命打击。

## 4 雷达装甲

雷达防护系统中的密集阵火炮与反辐射导弹、巡航导弹、航空炸弹交战的时间很短,只有0.1秒~1.2秒,交战半球半径只有50米~1500米,导弹或航空炸弹被密集阵炮火击中爆炸后,其部分碎片仍然会以较高的速度撒向雷达天线,因此要对雷达天线加装甲。目前,世界上已有碳纤维合成材料,可以抗击距离20米内,初速为900米/秒的高射机枪射击,其强度优于钢铁,对波长为厘米的电磁波的透波性能优良,试验表明对雷达性能基本没有影响。碳纤维合成材料已用于坦克装甲和舰艇甲板,可以做成雷达天线装甲。

## 5 雷达坑道

坑道对于雷达和雷达操作人员的防护是极其重要的。雷达坑道必须有防核防化功能。特别是由于现代精确制导钻地弹的出现,坑道的深度必须足够深。由于雷达发射机受波导长度的限制,雷达发射



机只能建在离地面十几米深度的地方，难于抗击现代钻地弹的攻击。但雷达显控台和操作人员可以放置在几百米深的地下坑道内（山脚下的坑道），可以通过光纤网络从几千公里外的地下指挥所遥控操作，保证人员的安全。

## 6 结束语

从最近的几场战争统计，航空弹药的使用占弹药使用总量的 85%。也就是说，作战使用的投弹兵器主要是飞机和导弹。为了夺取制信息权，总是首

先进行空袭。空袭中的首要目标是防空雷达（如对空、对海警戒雷达）。打开防空预警缺口，进而打击通信、控制与指挥中心等重要目标。空中打击是作战的主要形式。因此，反空袭是未来信息化战争的重要任务。雷达是防空系统的重要部件，是整个系统的“眼睛”，必须加以重点保护。必须彻底改变雷达无需防护和无法防护的观念。防空系统中的每一部地基雷达（如岸对海警戒雷达、对空警戒雷达）都应当配备雷达防护系统，加装装甲，建设牢靠的雷达坑道，从而保障海空雷达预警系统的安全，保证夺取信息化战争条件下局部战争的胜利。

## 参考文献

- [1] 向敬成. 雷达系统.北京：解放军出版社，2005：9
- [2] 陈东祥. 台湾高技术武器装备发展及作战能力研究.北京：国防大学出版社，2004：9
- [3] 中国人民解放军军事科学院战争理论研究部《孙子》注释小组.孙子兵法新注.北京：中华书局，1977：1
- [4] 梅遂生.光电子技术.北京：国防工业出版社，1999：9
- [5] 中国航天工业总公司《世界导弹大全》修订委员会.世界导弹大全（修订版）.北京：军事科学出版社，1998：1
- [6] 高技术武器装备知识手册.北京：国防工业出版社，2002：3

## 作者联系方式

通信地址：海军指挥学院浦口分院三室海军指挥学院信息战研究系

邮政编码：211800

联系电话：13951980663 025-80843232



# 基于分数阶傅立叶变换的频谱共享通信方案

肖涵 刘榕 吴春

**摘 要:** 文章主要介绍了分数阶傅里叶变换的基本概念和原理, 分析了线性调频信号在分数阶傅里叶变换中的特点, 从而利用分数阶傅里叶变换对线性调频信号的进行检测和解调, 提出一种在已有通信信号背景下实现频谱共享的通信方案, 并进行计算机仿真, 结果表明这种方案具有一定的实际意义。

**关键词:** 分数阶傅立叶变换; 线性调频; 频谱共享; 直接序列扩频

## 1 引言

随着无线通信技术的发展, 无线环境日益复杂, 频谱资源日益紧张。如何在高效利用频谱资源的同时, 提高通信信号的抗截获、抗干扰能力已成为目前通信研究的一个热点。通过扩展通信频谱, 降低单位频谱内的信号能量, 采用各种的变换, 提取有用信号, 消除干扰, 改善了自身通信质量已成为目前通信研究的一个重要方面, 并得到广泛引用。线性调频信号是一种具有低截获概率的信号。其时域表现为非平稳扫频信号, 在分数阶傅里叶变换域里则呈现明显的聚焦特性<sup>[4][5]</sup>, 而普通调制信号(如 QPSK, FSK 等)并不具备这样的特性。据此本文提出了一种在常规通信信号背景下来传输线性调频信号的通信方案, 从而实现频谱资源的高效利用, 同时提高信息的抗毁性和抗截获能力。

## 2 分数阶傅里叶变换简介[4]

分数阶傅里叶变换(Fractional Fourier Transform, FRFT)作为 Fourier 变换的一种广义形式, 信号  $x(t)$  的分数阶傅里叶变换定义为:

$$X_a(u) = \int_{-\infty}^{+\infty} k(a, t, u) x(t) dt \quad \text{其中,}$$
  

$$k(a, t, u) = \sqrt{1 - j \cot a} \exp[j\pi u^2 \cot a + j\pi t^2 \cot a - 2j\pi ut \csc a]$$
 令  $a = p\pi/2$ ,  $p \neq 2n$ ,  $n$  是整数, 并称  $p$  为分数阶傅里叶变换的阶。

它可以解释为信号在时频平面内坐标轴绕原点逆时针旋转任意角度后构成的分数阶 Fourier 域上的表示方法。信号的 Fourier 变换可看成将其在时间轴上逆时针旋转  $\pi/2$  到频率轴上的表示, 则

FRFT 可以看成将信号在时间轴上逆时针旋转任意角度到  $u$  轴上的表示( $u$  轴被称为分数阶 Fourier 域)。

## 3 线性调频信号的分数阶傅里叶变换

如果发射的射频脉冲信号在一个周期内, 其载频的频率作线性变化, 则称为线性调频(LFM), 它是一种典型的非平稳信号<sup>[1][3][4]</sup>。

比较 RWT 和分数阶傅里叶变换功率谱的表达式<sup>[6]</sup>, 我们可以得到:

$$|X_a(u)|^2 = 2\pi D_x(u, a) \Big|_{\substack{m = -2\pi \cot a \\ \omega_o = 2\pi u \csc a}}$$

这也正是信号分数阶傅里叶变换的模平方正好是该方向上的 RWT, 所以, LFM 信号  $\exp[j(\omega_o t + \frac{1}{2} m t^2)]$  的 RWT 会在对应的参数  $(m, \omega_o)$  处出现尖峰, 如: 一个 LFM 信号  $s(t) = \exp(j10\pi t + j5\pi t^2)$  在适当的分数阶傅里叶域中将表现为一个冲击函数, 呈现出能量的高度的聚集, 如图 1 所示, 根据这一特点, 可估计出 LFM 信号  $\exp[j(\omega_o t + \frac{1}{2} m t^2)]$  的参数为:  
 $\omega_o = 2\pi u \csc a$  ;  $m = -2\pi \cot a$

## 4 基于FRFT的频谱共享通信方案[6]

为简单起见, 本方案以 BPSK-DSSS 信号为例, 发送端同时发送 BPSK-DSSS 信号和数字调制 LFM 信号(数字信号 1 或 -1 控制 LFM 信号的调频率), 接收端对各自信号进行解调, 对 BPSK-DSSS 和 LFM 信号分别解调, 从而实现在存在其他

同频信号的背景下的信息提取。系统方案如下图 2 所示。

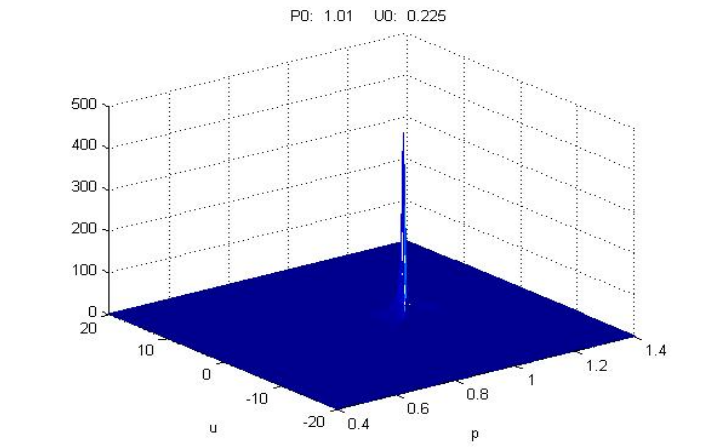


图 1

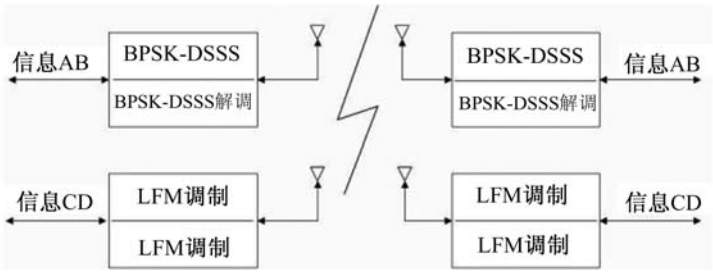


图 2

图中信息 AB 和信息 CD 可以是同一个用户的信息，也可以是不同用户的信息。为了简单起见，在仿真中采用前一种情况，两种不同调制格式的信息由同一个用户发送。

5 实现方法

发送端只需将两类信息分别进行调制，然后在同一频率分别发送即可（这里当然要求 BPSK-DSSS 和 LFM 信号处于同一频段否则就谈不上频谱共享了）。接收端对 LFM 信号的解调采用分数阶傅立叶变换实现信息检测，BPSK-DSSS 信号作为干扰出现在背景中；对有用 BPSK-DSSS 信号而言，LFM 信号相当于扫频干扰，解调前可以对 LFM 信号进行干扰抑制，方法即文献<sup>[6]</sup>中的看干扰滤波，只是在本文中为带阻滤波器。由于 DSSS 本身具有一定的抗干扰能力，当 LFM 信号功率不是很大的时候，根本不需要进行干扰抑制也可以获得较为理想的性能，这一点从下面的仿真中可以看出。

6 计算机仿真

本文对仿真模型作了如下简化：只考虑信息的单向传输，不考虑多经影响，理想 AWGN 信道，PN 序列默认同步，通信调制参数为收发双方默认参数，BPSK-DSSS 信号和 LFM 信号载波频率相同，对直接序列扩频信号进行常规相关解调，而对 LFM 信号采用变换域调频率检测方法。

扩频因子 SF=128，线性调频信号调频率 u 分为 32 和 64 两种情况，从扫频带宽角度来理解，前者扫频 DSSS 信号带宽的一半，后者扫频整个 DSSS 信号带宽。如图 3 所示，其中 0.5 表示归一化奈奎斯特频率，正斜率表示发送符号 1，负则发送-1。

为了比较 LFM 与其他调制信号与 BPSK-DSSS 信号实现频谱共享的优势，本文对普通 BPSK 与 BPSK-DSSS 共存进行了仿真，如图 4 所示。从仿真结果来看，在信噪比相同的情况下，根本无法实现 BPSK 通信，换句话说，无法实现 BPSK 与 BPSK-DSSS 信号频谱共享。

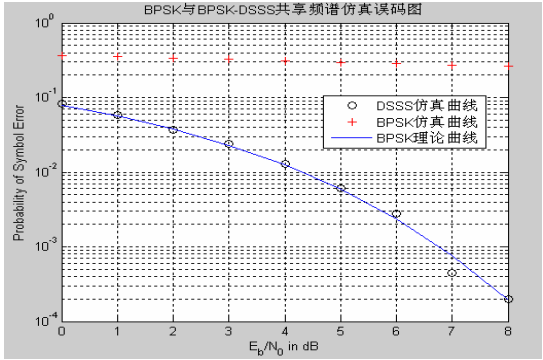
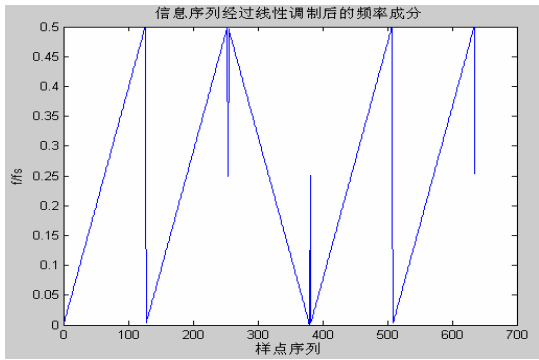


图 3

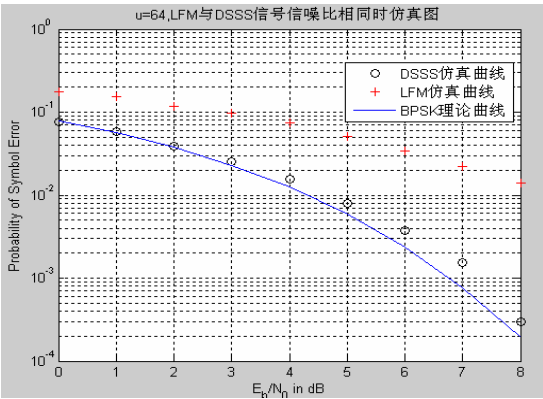
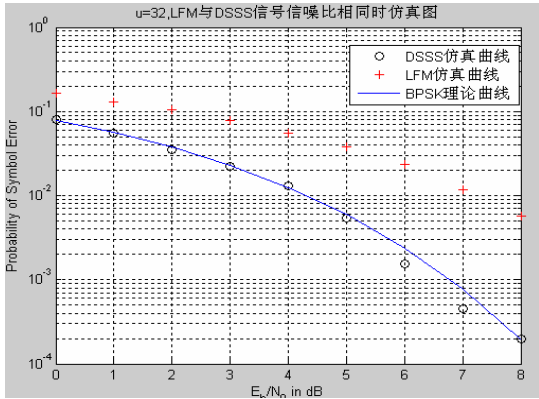


图 4

当采用 LFM 信号与 BPSK-DSSS 进行频谱共享是，对于每一个  $u$  值，分别进行仿真，如图 5 所示，此是在 BPSK-DSSS 与 LFM 信号为相同信噪比时的仿真结果。

图 5 为将 LFM 信号功率增加 3dB 的仿真结果，可见 LFM 信号的误码率得到明显的改善，但

是 BPSK-DSSS 的误码率受到了恶化。通过仿真中当 LFM 信号比 BPSK-DSSS 信号的信噪比高 6dB 时，对于 LFM 信号来说几乎检测不到错误。从图中我们还可以看出就算在同样功率情况下，扫频带宽越宽，对直接序列扩频信号的干扰越严重。

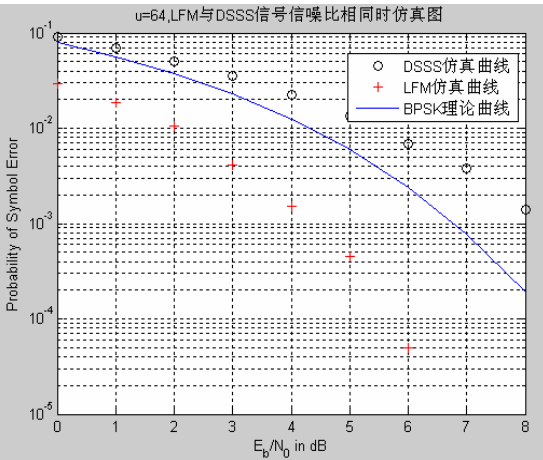
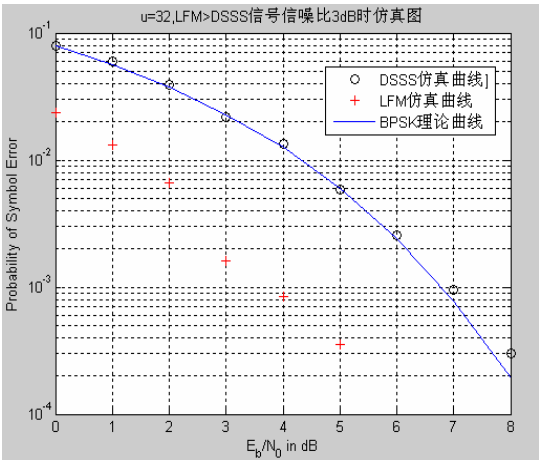


图 5

图 6 分别为没有 LFM 信号和加上 LFM 信号后的信号频谱。由图可见，利用传统的傅立叶变换谱，观察不到任何关于 LFM 信号的特征，实现了

对信号一定程度的隐藏。另外就算是利用分数阶傅立叶变换，当阶次不很接近的情况下也很难发现 LFM 信号的存在。

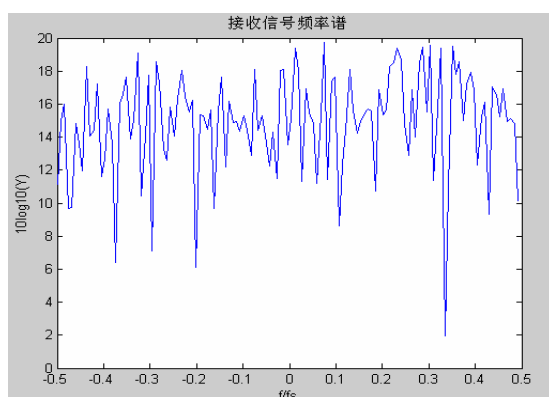
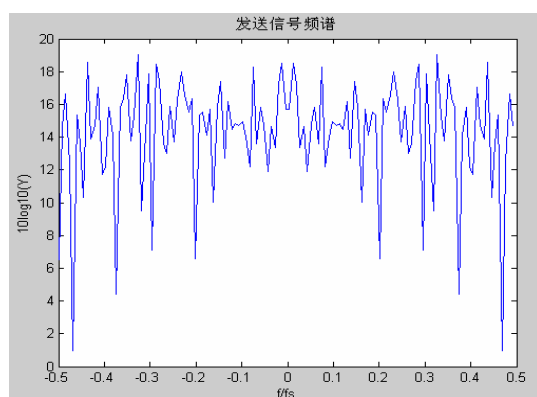


图 6

图 7 分别为调制输出端 LFM 信号和接收端受

到污染的 LFM 信号的 FRFT 谱图。

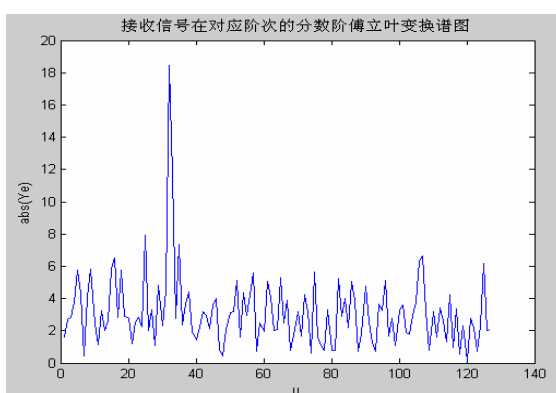
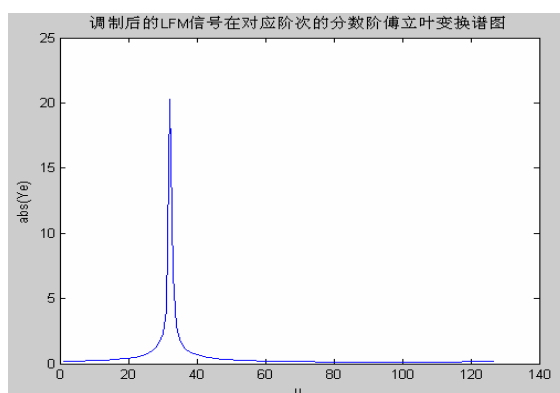


图 7

可见 BPSK-DSSS 信号与噪声一样在数阶域不出现能量聚集，体现为噪声特性。这就是利用 LFM 提高通信信号抗截获能力的理论基础，同样，在对 LFM 信号进行解调时也是利用了其在分数阶域能量聚集的位置来实现信号检测。

由仿真结果可以看出，在具有一定的抗截获能力的基础上实现频谱共享，LFM 调制较之普通 BPSK 调制具有较好的误码性能，在共享频谱信号信噪比相同的情况下，BPSK 信号根本无法进行通信，而采用 LFM 调制却具有相当好的性能。由于对 LFM 信号的解调采用的是非传统的方式，而是在变换域进行信号检测（傅立叶频谱中无法看到 LFM 信号的特征），从而提高了 LFM 信号的抗截获能力，实现了在较高抗截获能力的同时提高了频谱资源的利用率。

谱资源的利用率。

## 7 结束语

本文利用分数阶傅立叶变换理论以及线性调频信号的 FRFT 特性，提出了在 BPSK-DSSS 宽带信号下面实现 LFM 信号共享通信的系统方案，并建立仿真模型。通过 Matlab 仿真，证实了基于 FRFT 的频谱共享通信的可行性。同时由于模型作了很多简化，在实际应用中还有很多工作要做，比如序列同步，参数选择等，都有待于进一步的研究和探讨。

### 作者联系方式

通信地址：解放军理工大学通信工程学院研究生二队

邮政编码：210007

联系方式：010-66820129

# 防空导弹网络化作战关键技术研究

熊新平 沈丽艳 宋晋敏

**摘 要:** 在分析了现代空袭威胁环境对防空导弹武器系统的新威胁后,提出了一种新的防空导弹武器系统网络化体系结构,重点分析了防空导弹网路化作战的关键技术和可能的解决途径,对几种典型制导体制的防空导弹可能实现的网络化作战样式进行了分析。

**关键词:** 空袭体系; 防空导弹; 网络化; 体系结构; 作战样式

## 1 引言

随着信息化时代的到来,现代战争的形态发生了根本性的变化。军事强国的空袭体系利用一体化的指挥和控制、隐身和电子干扰、反辐射攻击、防区外攻击、低空超低空攻击、超饱和攻击、精确打击等多种手段,空袭作战已实现体系化、信息化、网络化,实现了对移动和时敏目标的精确定位和快速瞄准,并提供实时火控支援。美国研制的战术目标瞄准网络 TTNT,是一个数据传输量大、反应时间短,从传感器到射手的高速动态网,在目标探测、主动识别、瞄准、达到交战标准、打击和损伤评估的全过程,都利用 TTNT 提供及时有效的信息,从战区内的任何设备获取实时信息,打击移动目标,达到了极高的作战效能。

传统的防空导弹都是层次化指挥控制,以发射平台为中心进行防空作战的,防空导弹火力单元内指挥控制系统、制导雷达、发射装置和导弹等各作战装备之间存在着固定的隶属关系,信息贡献程度低、资源不能互操作,不能适时重组,如火力单元指控系统或制导雷达被击毁,则整个火力单元失去作战能力;如果战术单元指控系统被毁,则其所管辖的各火力单元转入自主作战模式,不可避免地出现重复射击和漏射击的情况,作战效能较低。现有防空导弹杀伤区与制导雷达方位向保精度扫描扇面不匹配,火力单元配属制导雷达限制了制导能力的发挥;同样,面对空中目标的超视距攻击,防空导弹火力单元制导雷达不能发现目标,致使导弹无法形成作战能力。现有防空导弹武器难以应对空袭体系饱和攻击,综合电子对抗能力受极大压制。

防空导弹网络化为从防空体系层面提升防空导弹的作战能力以及整个防空体系作战效能带来了极

大的发展机遇。

## 2 国外相关研究概况

美国依靠其强大的信息技术优势,在武器系统信息化、网络中心战等方面都走在世界前列。

美国海军提出的“网络中心战”的作战结构由三级互连互通互操作的作战网络组成:第一级为联合合成跟踪网,主要依赖于 CEC,用于武器控制;第二级为联合数据网,主要依赖于 Link-16/11,用于部队控制;第三级为联合计划网,主要依赖于 IT-21、GCCS 等,用于部队协调。CEC 系统主要由协同交战处理机(CEP)和数据分发系统(DDS)组成。CEP 主要负责跟踪大量空中目标(航迹管理和更新);在舰队的运动平台之间保持精确的联网定位(网格锁定);进行数据相关、航迹合成、组合识别。DDS 主要负责自动建立网络,把关键传感器数据近实时地分发给舰队所有成员,供所有平台使用。2000 年以后 CEC 系统投入应用和不段改进,已验证了其超视距拦截,多目标联合跟踪,弹道导弹合成跟踪能力。

为了有效对付低空超低空飞行的巡航导弹的威胁,美国陆军委托洛克希德-马丁公司开发了“联合对地攻击巡航导弹防御架高的联合探测器”JLENS 项目。JLENS 由两部远程监视雷达和高性能火控雷达构成,分别搭载于两个 71 米长、悬空高度约 4572 米的浮空器上。JLENS 可与爱国者导弹、标准导弹、SLAMRAAM 等多种防空导弹系统协同工作;侦察雷达可侦测到 250km 内的敌机和巡航导弹,通过多传感器、指控通信和情报网提供全方位集成空情图;火控雷达可在防御区域内同时跟踪多个目标,并提供来袭敌机和导弹的精确位置

图像,实现动平台异地制导。采用 JLENS 后,使防空导弹的杀伤区基本不受地球曲率、地形遮挡和目标 RCS 下降的变化,防空作战效能大幅度提高。

俄罗斯强调防空导弹射程和火力密度需加强,网络化作战是重要的发展方向。在 C-400 防空导弹平台上,设想将现有的空基、海基、地基、天基信息源综合,但导弹发射和制导仍在火力单元内完成;还要加上空中预警机;同时实现火力单元外对导弹的发射和制导控制;通过上述信息源,实现空空导弹和地空导弹的一体化作战,实现歼击机对地空导弹的制导。

### 3 防空导弹网络化体系结构

#### 3.1 防空导弹网络化体系结构组成

防空导弹网络化作战的根本目的是提高防空导弹武器系统的信息质量和信息利用程度,最大限度地提升防空导弹的作战效能,提升防空体系应对现代战争威胁的整体作战效能。为了实现上述目的,要求购建一全新的网络化作战体系结构。该体系结构由作战管理/指挥控制系统网络、跟踪制导网络、防空导弹网络、区域通信网络互连组成,是一个信息共享、资源互操作的高效的防空体系。

在网络化作战体系内,主要作战资源装备(包括指控系统、探测制导系统、发射架等)之间无固定的必然联系,只是在作战过程中根据需要动态组合起来完成一次防空作战任务,随着任务的结束,这种组合关系即告结束,资源释放,供下一次形成新的作战组合时使用。对目标的探测跟踪由空地一体化、多传感器组成的探测制导网络完成,提供全作战空域持续稳定的战场态势感知,目标信息质量应能满足导弹制导控制需要。各指挥控制系统软硬件组成一致,功能相同,指控可变中心,系统具有扁平化的特征,资源优化程度更高,反应时间更短。在统一信息场的支持下,通过优化的战术使用方式和作战资源组合方式,实现协同探测、协调交战决策、超视距拦截和接力拦截等崭新的防空作战模式。

#### 3.2 网络化作战体系结构特点

网络化作战体系结构特点主要体现在协同探

测、信息共享与协同指挥控制几个方面。

多谱段、多体制、空地一体探测制导系统通过战术数据链网状互联。当前指控中心节点根据目标空域分布特性和种类,实时组合成不同的探测跟踪网络。通过探测跟踪系统组网协同探测,在缩短系统反应时间、使导弹制导可利用信息范围增大、作战可用性增强、扩展空间覆盖范围、改善探测、跟踪性能等方面获得优势,为导弹能力的最大发挥提供可能。

在网络化体系结构防空导弹武器系统中,指挥控制系统具有鲜明的特点,一是可根据空袭模式,组织现有作战资源,动态形成作战组合,最大限度地发挥武器系统的作战性能;二是可以适时切换指挥中心,当发挥指挥功能的指控中心发生故障或被摧毁的情况下,网络化体系结构防空导弹武器系统可根据当前作战形势和一定的判断准则,动态地将指控中心切换到功能完好的其他指挥节点,从而可以有效提高武器系统的战场生存能力,避免出现重复射击和漏射击情况,最大限度地提高防空作战效能。

#### 3.3 防空导弹制导体制与网络化作战样式

采用无线电遥控体制的防空导弹武器系统一般采用目标-导弹相对测量形成制导指令,网络化作战样式相对有限。

TVM 制导系统是通过地面雷达发射照射信号,目标反射信号一路直接到达地面雷达;另一路被弹上系统接收,获得目标信息通过下行线转发到地面;再对地面雷达直接收到的目标信息与通过 TVM 获得的目标信息进行相关处理,形成制导控制指令。这种体制的网络化作战能力较强,具有反低空突防作战样式,反低空作战能力得到加强。TVM 制导体制防空导弹武器系统具有实现提示交战和远程交战能力。

捷联惯导/指令修正+自动寻的的复合制导体制武器系统的作战特点是具有导弹自主定位、利用外部信息自主解算制导控制指令的能力,因此这种体制导弹武器系统拦截高度高、作战斜距大。根据目前的技术状态,在一定拦截空域内,可实现网络化作战异地制导;但在高远拦截空域上尚有一定问题,还需要研究减小探测跟踪制导网系统误差、导弹初始对准误差以及导引头预定误差方法,以及新的导引头体制,在全空域范围实现异地制导。

### 3.4 网络化作战体系作战过程

网络化体系结构防空导弹武器系统与现有体系结构防空导弹武器系统作战过程相比,有很多显著的特点。

网络化体系结构下,每个指挥控制节点既具有战术单位指控系统(以下简称指控中心节点)功能,又具有火力单元指控系统(以下简称本地指控节点)功能。网络化防空作战过程是由当前指定的指控中心节点进行统一指挥;当指控中心节点出现故障或被毁时,按照战前确定的替代准则,由其他的某个本地指控节点行使指控中心节点功能。可根据当前指控中心节点确定的网络化作战样式,通过对各探测制导系统进行动态组合和资源的合理调度,形成相应的探测制导网络,提高对目标的探测跟踪质量,扩大跟踪覆盖范围。当前指控中心节点根据战场态势和体系内资源可用情况等,适时形成若干个由本地指控节点、探测制导网、发射装置和拦截导弹的动态作战组合。

## 4 防空导弹网络化的关键技术

### 4.1 浮空平台系统技术

受微波视距传输的限制,地基探测制导系统发现不了视距外空袭目标,使得导弹难以在远距离上拦截低空超低空突防目标,导弹的作战能力得不到有效发挥;同样,地域网必须设置多个中继站实现大范围防御区域内的通信,通信设备量激增、通信时延与可靠性等问题突出。网络化作战系统配置浮空平台的根本目的是搭载目标探测系统和通信中继电台,解决低空超低空飞行目标探测问题以及防御区域内通信中继问题。

浮空探测器用以实现对多目标的全方位的搜索、跟踪与对拦截导弹的制导。它采用地面电缆供电、脉冲多普勒技术实现对强地杂波下的小目标检测。浮空通信电台可以作为区域防空网络化作战系统通信链路的中继节点,用于实现全区域范围目标信息分发。

### 4.2 时空一致性技术

网络化体系结构防空导弹武器系统要求各作战装备必须在统一的时间和空间尺度上工作,因此时

空一致性研究倍受人们关注。

网络化作战系统中各探测跟踪系统为了协同作战,特别是在多基地测量的情况下,需要进行严格的时间同步,这样多基地测量系统才能够正常接收到信号,解算出多基地测量系统的目标定位信息,为射击诸元计算提供数据和形成制导指令。由于各探测跟踪系统对同一目标的测量数据的测量时刻不一致、以及探测跟踪系统与网络化作战信息融合处理系统之间存在信号传输延迟等因素,要求各传感器必须在每一空间点的测量数据之前加上时标,同时也要求网络化作战信息融合处理系统在进行数据融合时进行时间对准处理。

探测跟踪系统的精确定位定向是网络化作战点迹合成与数据融合的基础。因而网络化系统的空间一致性也成为制约网络化作战系统是否能够形成精确的战场态势和形成协同作战能力的关键的技术。

### 4.3 指挥控制功能动态重组技术

指挥节点指挥控制权的动态转移能力是指在作战过程中如果指挥节点出现被毁、故障、通信中断等情况,指挥控制的权限可以不降级地转移到其他指挥控制节点,确保每个时刻都有一个指挥中心统一控制整个防空作战过程,避免出现重复射击和漏射击的情况。随着计算机和通信网络性能的不提高和价格的不断下降,可以使得网络化体系结构防空导弹武器系统内各个指挥控制系统配置相同的软硬件环境,从而确保各指挥控制系统具有相同的战场态势、相同的指挥控制能力,为指挥控制权的转移奠定了基础。

在统一信息场的支援下,对目标的拦截不不需要自身的制导雷达发现跟踪目标,也不仅仅是自身一部雷达截获跟踪和制导导弹,而是形成动态的作战组合。如A营制导雷达出现故障或被毁,B营部分发射装置被毁或出现故障或导弹耗尽,现有体系结构下A营发射装置及其导弹不能投入战斗,而B营制导雷达制导能力过剩;在网络化体系结构下,则可利用B营制导雷达制导A营防空导弹,使防空导弹武器系统能持续地投入防空作战,保证一定的火力通道,提高了作战效能。

### 4.4 探测制导网资源调度技术

为建立统一的信息场,必须对目标探测跟踪网络进行统一的调度,适时组成针对饱和攻击目标、



干扰目标、隐身目标、低空超低空目标的探测跟踪网络,为网络化体系结构防空导弹武器系统提供及时、准确、稳定、统一的空情信息场和制导指令场。

对探测器进行组合,统一进行资源调度与数据处理策略,保证对饱和攻击目标流中的每一个有威胁的目标进行精密跟踪测量;浮空探测器能够对低空飞行目标在远距离发现并进行跟踪,通过空地一体化主被动探测网络,来保证对有威胁的低空飞行目标进行精密跟踪测量;通过多谱段、多体制的协同探测方式,来保证对隐身目标和干扰目标进行远距离持续跟踪测量,形成指控系统所需的火控信息。

首先建立目标排序的优先级准则,对各类因素赋予一定的权系数,通过加权平均计算目标的优先级,作为探测制导网络资源调度的依据之一。在目标排序基础上同时还要考虑当前探测制导系统的技术状态。在目标威胁排序和综合考虑探测制导系统当前技术状态的基础上,按照分配时机、目标分配的优先级、探测制导系统覆盖区、目标通道数约束、以及探测器与目标相对位置关系准则进行目标分配。

## 4.5 点迹合成与信息融合技术

在空地一体化协同探测中需要研究目标点迹合成方法,开展相应的制导精度分析与误差补偿研究,特别是解决目标同一性识别问题。

信息融合技术是对多个不同探测制导系统探测的同一个目标的定位信息和属性识别结果进行融合,从而改善对目标的跟踪与识别质量,特别是当某个探测制导系统对目标跟踪丢失或跟踪时断时续的情况下实现航迹接续,以及当某个探测制导系统对目标属性判断不明的情况下实现正确判断以免造成错误拦截。

数据预处理是信息融合的重要步骤,包括进行坐标变换和时间对准,数据的分类处理以及航迹关联与同一性判别等。应采用分布式数据融合结构,加权最小二乘法对各雷达的滤波值进行加权融合,这样可以降低网络通信传输数据量和数据融合运算量。利用证据理论中的 Dempster 组合规则,进行时空序贯融合,给出目标属性判别结果。

## 4.6 区域通信网络技术

网络化体系结构防空导弹武器系统中的通信系统,需要传送的信息一般可分为三类,包括预警探测信息,指挥控制信息,探测制导信息。

预警信息传输距离远,传输速率和带宽要求不高,一般采用微波中继或散射通信的方式进行传输。传输距离较远,可达上千公里。指挥控制信息主要包括对作战指挥信息,战前计划信息,雷达控制指令,武器控制指令;指挥控制信息传输距离一般为 30~100km 左右,传输带宽要求至少 1MHz,采用超短波方式组网,实现一点对多点大容量通信,通信节点数为 30 个左右。探测制导信息主要包括对导弹和目标的探测数据,对导弹的制导数据;传输手段为结合数据分发功能的多功能相控阵雷达,以及新开发的具有 CEC 初步功能的 MCE 设备;信息传输速率一般在 2~10Hz,带宽要求至少 4MHz,通信距离为 100Km 左右。该级节点数一般为 20~50 个左右。

通信网络子系统由远程通信网(预警信息网络)、地域通信网(网络化体系结构防空导弹武器系统区域通信网络)和局域网(指控节点内部通信网络)三部分组成,采用分布式网络结构,迂回路由方式,传输信道采用数字微波机、散射信道、卫星信道以及有线信道等方式。同时,可提供多种接口来满足不同防空导弹武器系统的接入要求。

指挥中心动态可变的技术要求武器系统中不存在明显的指挥中心节点,即武器系统的生存能力不依赖于某一个中心。这就要求在网络化作战系统的通信组网方式具有无中心节点的能力,所有的作战设备都通过网络挂接在系统中,作战信息通过网络相互分发,并保持作战能力,在网络上某个节点受到损害时,武器系统的整体作战能力没有明显下降,而且在理想的方式下,应该有相应的指挥节点代替执行指挥功能。

实现“扁平式”的指挥结构,需要依赖大量信息的快速传输和共享,这就要求必须发展高速数据传输技术。

## 5 结束语

战术防空导弹向网络化体系发展,是军事需求和技术推动的共同产物,是战术防空导弹体系一个



重要的发展方向,可直接支持新一代网络化体系结构的区域防空导弹武器系统的总体方案论证和关键技术研究,应用于现役和在研的防空导弹武器系统的信息化改造,带动相关分系统关键技术的攻关以及推动精确制导技术、雷达探测技术、导航与控制技术、指挥控制通信技术、系统仿真技术等相关专业技术的发展。

应在防空反导领域尽早、分步开展网络化作战系统和技术的研究工作。近期,开展混编防空导弹组网作战系统工程研制,通过区域通信网络,改造各防空导弹火力单元的接口,实现互联互通,传感

器信息航迹融合,指挥调度信息共享,提高作战效能。中期,开展武器控制级防空网络化作战系统研究,立足防空导弹火力单元格局,在无中心通信网络上,以制导信息网络化、协同制导为目标,实现制导雷达协同探测、超视距拦截、异地制导等崭新作战模式,提高防空作战效能。远期,实现可动态重组的、扁平化、资源优化型的防空反导一体化作战体系,作战指挥扁平化、可变中心化,系统可以动态重组,资源分配在作战装备层面进行,最大限度地提高作战效能。

### 参考文献

- [1] 殷兴良,网络化防空反导作战系统设计与演示[A].网络化作战技术文集(特辑)[C],北京:现代防御技术编辑部.2004.
- [2] 殷兴良,论新一代防空导弹的体系化武器系统[A].防空导弹体系论文集(第七集)[C].北京:现代防御技术编辑部.2005.
- [3] 徐品高,三道防线和网络化中心战是当前防空领域的重大军事和技术变革[A].防空导弹体系论文集(第七集)[C].北京:现代防御技术编辑部.2005.

### 作者联系方式

通信地址:北京市142信箱15分箱

邮政编码:100854

联系电话:13366063732

# 军事大系统中的监控系统体系结构与关键技术

杨雪南 丁武将

**摘 要：**随着军队信息系统的建设，对信息系统的监控，从而确保信息系统良好运行十分重要。本文首先概要描述了面向军事信息系统的监控系统需求，阐述了监控系统的体系结构，详细分析了体系结构中的数据采集层、数据处理层和数据展示层，最后，探讨了监控系统中的关键技术。

**关键词：**体系结构；网络管理；综合监控；网络管理

## 1 前言

随着科技进步、战略需求和战争实践，军队信息化建设已成为部队现代化建设的重要内容，而军事信息系统则是军队信息化建设的重要组成部分。军事信息系统组成复杂、IT 环境多样，可靠性、实时性、性能要求很高，如何保障军事信息系统的可靠、稳定运行是我们面临的一个重大问题。

为解决这一问题，就必须能及时掌握军事信息系统运行过程中的各种运行状态信息，并对这些状态信息进行分析，判断当前运行状态是否正常。目前，我军这一工作许多都依靠人工进行，缺乏自动化手段。手工方式不仅发现问题的及时性差，而且工作量大，重复性劳动强度高，对人员的技术要求高。国外的一些网管产品，如 HP Openview、BMC Patrol、IBM Tivoli 等，在可使用性、可维护性、价格等许多方面难以满足我军需要，即便购买了产品和服务，往往也难以用起来（国内其他行业用户也是如此）。

因此，为有效保障军事信息系统可靠、稳定运行，及时发现并排除系统运行过程中发生的各种故障，迫切需要提供军事信息系统的自动监控手段，通过自动化的监控系统，全面掌握系统的运行状态，一旦出现故障或性能问题，能立即报警，通知系统维护人员，并进行相应处理，将故障带来的影响降到最小，从而提高军事信息系统的可靠性、稳定性。

## 2 需求分析

### 2.1 范围与功能

监控系统需要监控的对象或者说需要监控网元可分两大类，一是平台类，包括各类主机

（HP\_UX, AIX, Solaris, Linux, Windows 等）、数据库、中间件、网络、存储、备份，二是应用层网元，包括各个军事信息应用软件。监控系统的主要功能要求如下。

1) 监控系统能将军事信息系统的运行状况通过直观的界面展示出来，及时发现平台层和军事信息系统应用层的各种告警，并对告警进行分析，进行故障定位。

2) 监控系统能对当前及历史告警信息进行综合查询、分析，发现系统最薄弱环节，为更好地进行军事信息系统的运行维护提供帮助。

3) 监控系统能对军事信息系统运行的各种性能进行分析、展示，从而为系统的扩容、新军事信息系统的规划提供可靠的依据。

4) 监控系统能提供知识库支持，方便运行维护人员进行故障的精确诊断、定位，以及故障的及时、快速处理。

5) 发生告警时，监控系统能提供包括短信、邮件等在内的通知手段。

### 2.2 主要监控指标

1) 主机设备。主机设备的主要指标包括主机设备的运行状态、CPU、内存、磁盘、文件系统、进程、配置信息。

2) 网络设备。网络设备（核心交换机、SAN 交换机、防火墙等）的主要指标包括网络设备的运行状态、网络流量、配置信息。

3) 数据库。数据库的指标主要包括数据库的工作状态、数据库自身告警和报警信息、数据库表空间的使用情况、数据库的进程状态、数据库的内存利用状态、数据库表空间的读写命中率、数据文件或数据备份的读写命中率、数据库碎片的情况、

数据库特定表的空间信息、数据库日志空间的使用情况、数据库版本信息等的管理。

4) 中间件。中间件 (Websphere、Weblogic、Tuxedo 等) 的指标与具体的中间件产品有关, 如 Weblogic 的只要指标有连接池、服务器数量和状态、执行队列等。

5) 存储设备。存储设备硬件状态指标, 如运行状态、硬盘状态、磁盘通道状态、存储 CACHE 读写命中率、其他部件 (风扇、电源模块等) 状态等; 配置属性指标如存储阵列数目、存储阵列标识、存储阵列类型、存储配置容量、存储采用的 RAID 方式等。

6) 备份设备。主要有三部分。备份软件状态指标包括各进程状态、进行数据备份的进程状态、备份结果等状态; 备份资源占用指标包括备份进程占用 CPU 资源、内存资源利用率; 备份硬件配置属性包括介质库标识、类型、数目、容量、微码版本、驱动器标识、类型、数目; 数据通道标识、类型、数目、微码版本。

(7) 军事信息应用软件。对应用软件运行的一些指标, 如日志、执行状态等。具体指标与具体的应用软件有关。

3 体系结构

体系结构主要由三部分组成: 包括数据采集层、处理层和展示层, 另外还包括系统管理和安全管理。监控系统的体系结构如下图 1 所示。

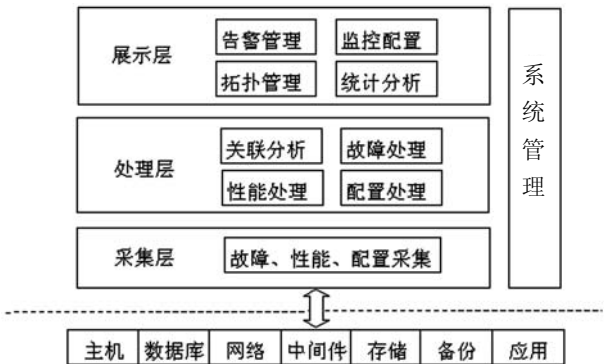


图 1 监控系统体系结构

数据采集层负责监控数据的采集, 将采集到的监控指标数据提交上层进行处理。

数据处理层从数据采集层接收各种监控对象的故障数据、性能数据和配置数据, 对这些数据进行

格式验证、存储, 并进行告警分析判断和告警通知。

监控展示层提供监控配置 (配置监控网元、监控信息点等)、监控信息展示功能。

系统管理和安全管理主要提供用户管理、权限管理、以及维护管理。

目前, 监控系统通常提供统一的基于浏览器的 B/S 接入访问方式, 方便系统的部署和使用、维护。

3.1 数据采集层

采集层是监控数据的来源, 监控数据包括故障数据、性能数据和配置数据, 也可分为平台数据 (包括主机、数据库、网络、中间件等) 和业务应用软件数据。数据采集层的主要功能是实现对监控对象的各类指标进行采集和汇总, 将采集到的各类指标纳入一个统一的数据模型, 以便屏蔽各监控对象的差异性, 并便于将来扩充; 同时数据采集层还需要具有可管理性, 能对采集的具体指标、采集周期、采集网元等进行管理。

3.2 数据处理层

数据处理层的主要作用是对来自采集层的各种数据进行告警分析判断。

3.2.1 告警数据处理

告警数据处理针对来自平台部件类和应用部件类的告警事件, 进行告警判断, 并进行告警关联分析 (包括告警过滤、告警排重、告警生机、告警前转等)。

(1) 告警判断

对来自采集层的监控数据, 根据数据的标识、相关的规则, 进行相应的数据转换、计算等操作, 判断是否满足告警条件。如果满足告警条件, 则将该告警、告警的类别、告警等级提交事件关联分析模块或引擎。

(2) 告警关联

告警过滤: 针对系统维护、系统重新启动等情况, 可设定过滤规则, 如某个网元、某一时段、某一告警, 过滤这些告警, 避免干扰。

告警排重: 对于已经发生过的告警, 避免一段时间内再次告警, 可以设置排重规则, 减少重复告警的干扰。

告警归并：对于告警之间存在关联关系的告警，则仅需要显示根源告警。

告警升级：对于当前告警，根据设定的告警升级规则（如：发生的次数，时间窗口），可以将其从较低的告警等级提升为较高的告警等级。

告警前转：系统提供告警前转功能，将告警信息以各种手段（手机短信、EMAIL、语音、声响等）转至指定的维护人员。

### 3.2.2 性能数据处理

#### （1）预处理

预处理是对采集来的原始数据进行格式转换、检错纠错，形成内部标准记录，支持比较灵活的格式转换配置和检错纠错配置。

#### （2）计算与汇总

对预处理后的数据进行必要的计算、汇总形成所需的性能指标。

#### （3）阈值告警分析

性能数据反映了系统的运行状况，是判别被管资源运行是否正常的键数据。性能数据一旦超出预先设定的阈值时，系统将触发一个告警（即性能告警），并将转入故障数据处理。系统应能提供设定/查询/修改/删除性能阈值的工具，可设多个阈值进行分级告警。系统也应能设置性能数据的取样时间间隔。告警的内容应能比较全面地描述该性能数据超出阈值的情况，方便分析、排除故障。

### 3.2.3 配置数据处理

将采集的网元配置数据与当前保存的配置数据进行比对，进行审核和一致性分析。

#### （1）合法性审核

配置数据合法性审核是依据网元对象配置信息的数据合法性约束规则，对配置数据本身的合法性进行审核。约束规则可有多种形式，如某个配置项非空、某个配置项只能在特定值域内取值、某个配置项值有唯一性限制等。

#### （2）一致性审核

监控系统应审核网元对象的当前配置信息与网元对象当前的实际配置信息的一致性，如不一致进行配置数据的及时更新，如定期执行或随机执行。

#### （3）自动更新

监控系统提供配置数据的自动更新功能。在配置数据动态采集方式下，当配置处理模块接收到最新的配置信息，系统应检测最新采集到的配置信息

与网管系统中当前保存的配置信息是否一致，如不一致，系统能够根据最新配置信息更新监控系统中当前保存的配置信息。

#### （4）手动更新

监控系统应提供方便灵活的界面，供维护人员以手动方式更改网元对象的配置信息。

## 3.3 数据展示层

数据展示层是运维人员进行监控配置、系统监控和管理的用户界面，提供用户完成日常监控工作和系统配置工作的手段，监控展示层主要提供告警管理、性能管理、拓扑编辑与监控、网元配置、告警配置、统计报表、系统管理等几大功能。

### 3.3.1 告警管理

告警管理应该对不同的用户显示其权限范围内的网元告警信息，告警管理提供完整、统一的告警监视界面，集中显示来自数据采集层和数据处理层经过相关处理后的告警事件，确保维护人员可以及时响应来自平台和应用系统的分级、分类的告警。

告警管理应能够提供列表形式的告警监视界面，使维护人员可以监视到被管资源的实时告警事件和处理后的告警事件，并对相关告警进行告警确认、清除等操作。同时，方便地查看到相应的知识，利于故障排除。

### 3.3.2 性能管理

性能管理能够查看性能指标的变化情况，发现性能变化的特点。系统应提供层次化的网元树状结构，方便用户选择所关注的网元，以及网元下监控的性能指标，选中某个指标后能以数据列表方式、图形方式显示性能数据。

### 3.3.3 拓扑监控

监控系统提供拓扑呈现的功能。拓扑呈现包括网络拓扑和应用拓扑。拓扑管理要求分层次地呈现业务系统所涉及的所有被管理资源的拓扑结构。系统应具有灵活的监视和编辑的功能，同时在性能、告警、配置等方面动态反映资源环境的变化。在拓扑节点上可以查看相应资源详细配置信息，包括基本数据与汇总数据。

#### （1）拓扑图编辑与监控

拓扑图上的被管理资源不仅包括业务系统内的

所有主机设备、数据库、中间件等，还应包括业务系统应用软件的拓扑呈现。对应用软件的拓扑呈现，应提供灵活的定制方式。可以通过鼠标拖拉方式对拓扑图进行编辑、修改，并可选用合适的图标显示不同的网元等。在监控模式下，自动定期刷新拓扑图上节点的状态，反映系统实际告警情况，当节点上发生告警时，在拓扑图上能实时地进行显示，采用相应等级告警颜色进行显示。

#### （2）业务拓扑图

应用拓扑视图：能以直观的图形方式展示军事业务处理流程或业务处理模块/环节。应用拓扑视图体现被管理资源分布和关联情况、当前告警情况。

### 3.3.4 网元配置管理

监控系统所监控的网元可以通过网元配置管理增加、修改、删除管理，并支持用户自定义的网元分组功能，便于用户选定自己关注的网元范围。

### 3.3.5 告警配置

告警配置的功能是完成告警定义和关联规则的配置，以及对告警定义模板的管理，通过告警配置，使得监控系统能够根据告警定义和关联规则完成告警的判断和关联分析，包括告警定义管理、阈值告警模板管理（为同类网元的告警配置提供方便）、关联规则定义管理。

## 4 关键技术

监控系统的关键技术主要有如下这些（但不限于）。

#### （1）关联分析技术

由于告警之间存在某些关联关系，监控系统监测到告警时，需要判断该告警是根源告警，还是由于其他原因引起的关联告警，并屏蔽关联告警。例如，运行于某台主机上的数据库，当主机宕机时，数据库也会发出告警。监控系统需要根据网元之间的固有关联关系、通过交互界面设置的某些归并规则，进行综合的分析。通常，关联是很复杂的，监控系统提供专门的基于规则的关联分析引擎进行关联分析。

#### （2）非结构化数据处理

在监控系统中，常常需要获取非结构化数据，

例如操作系统日志文件、应用软件的日志文件，在出现告警时方便查看具体信息。常见的非结构化数据的处理方式有：

第一，不关心其内容，直接收集并存储，由用户分析其内容。在这种情况下，监控系统作为一个平台，起到数据自动汇集的作用，降低用户的手工操作量

第二，判断特定的模式是否出现。在这种情况下，一般有两种结果，一种是用布尔值作为结果，如果特定的模式出现则为真，否则为假，另外一种是根据该布尔值截取日志上下文中的相关信息作为分析结果，如：根据特定的关键字“error”截取错误原因描述。

第三，对比多个非结构数据的符合度，如：文件内容是否一致。

对于非结构化数据，通常需要设计了专门的采集软件，并且在处理层、展示层能对非结构化数据进行专门处理。

#### （3）数据处理、存储

当需要监控的网元数量较大并且对监控的实时性要求较高时，采集的数据量会比较大。这对采集层这并不是什么问题，但对数据处理层则会构成比较大的压力。例如，对于一个 15 台主机、2 个数据库、4 个中间件的军事信息系统，每个指标的采集周期为 1 分钟，通常在处理层大约需要 2000 条/分钟的处理能力。如果军事信息系统的规模更大，是上述的十倍、几十倍，则需要处理的数据每分钟会达到数万条。因此，考虑到处理层的各种处理、数据存储，需要采用数据缓冲技术和并发处理技术。

通常采集的指标数据会保存到数据库中，通过 SQL 进行访问。但是，用于进行图形展示（如生成曲线图）时性能并不好，打开一个显示曲线图的页面时常有明显的等待时间。RRD（Round Robin Database）格式来存储图形数据则能大大提高图形的展示性能，并且有开源的代码可以利用。因此，通常需要在处理层进行数据存储时分别保存到数据库和 RRD 格式文件中。

随着时间的积累，数据库中的数据会越来越多，需要的存储空间会线性增长，但对一段时间前（如 1 个月）的数据通常不会要求很细，所以可以对历史数据进行压缩存储，例如将数据按小时、按天存储，以减少数据量。

（4）代理和无代理技术

监控数据采集通常有两种技术，即代理和无代理技术。代理技术在被监控的信息系统主机上安装采集程序，优点是采集的指标多，几乎不受限制，并可方便地定置开发，缺点是需要安装一个程序，某些情况下部署受到限制。无代理技术无需在被监控的信息系统主机上安装采集程序，一个集中的采集程序能够完成所有的数据采集，优点是部署简单，易维护，缺点是远程采集指标会受到限制，某

些指标在这种方式下无法采集得到。因此，一个监控系统最好能同时提供这两种技术，根据实际情况合理选用。

（5）界面展示技术

监控系统在进行数据展示、拓扑图的编辑、展示时，可以采用目前主流的 AJAX 技术，提高界面的人机交互的友好性，并采用主流图形标准，如 VML 和 SVG。下表对 VML 和 SVG 作一比较：

	VML	SVG
优点	在 IE 中工作非常好，无须额外插件，与普通 HTML 完全融合	是国际标准，是未来的发展方向，语法严格，表现力更强
缺点	只有 IE5.0 以上浏览器支持，是微软的标准，表现力稍有欠缺	IE 中需要额外的插件才能展示，与 HTML 整合不够紧密

5 结束语

本文探讨了监控系统的体系结构和一些关键技术，随着军事信息系统的建设和运用的不断深入，监控系统的重要性将越来越显著地显现出来，监控

系统自身也将会有更多的问题需要面对，包括预警、故障诊断、故障现场快照、监控系统自身的监控、与军事应用更紧密结合等都是值得进一步关注的。

参考文献（略）

作者联系方式

通信地址：北京市西城区北展北街华远企业号 D 座二层  
邮政编码：100044  
联系电话：13611106457      13311285580

# CDMA军用移动网络安全接入研究

叶季青 韩清 叶酉荪

**摘 要:** 本文在分析介绍 CDMA 用户识别定位技术的基础上, 针对敌方通过截取无线信号, 确定移动用户的位置和通话用户的身份的情况, 研究了 CDMA 军用移动网络安全接入问题, 提出了一种适合军队使用的 CDMA 安全子网, 在现有 CDMA 技术体制的基础上, 对 UMTS 的用户识别方法进行部分改进, 可有效解决在 CDMA 通信中敌方识别用户身份和用户定位的问题。

**关键词:** UMTS; TMSI; UTRAN; 识别定位

在无线通信领域, 由于空中接口都是开放的, 通信系统使用的空中传输介质是一种基于广播的介质, 在小区的任何地方, 窃密者都可以截取无线信号, 确定移动台的位置, 监听移动台的通话内容或是冒充合法移动台的身份。

## 1 UMTS用户识别定位的框架

UMTS (全球移动通信系统) 使用 CDMA (码分多址) 技术, 它是在 GSM/GPRS MAP 网络的基础上发展而来的, 除了在电路交换域和分组交换域的高层协议基本相同外, UMTS 的 USIM (通用用户识别模块) 也是从 GSM 的 SIM (用户识别模块) 发展而来的。

UMTS 由三大部分组成: CN (核心网)、RAN (无线接入网) 和 UE (用户设备), 核心网包含 CS (电路交换域) 和 PS (分组交换域), 无线接入网为 UTRAN (UMTS 地面接入网), 用户设备可以是手机或数据终端。UE 是基站 (Node B) 在空中接口的对端, UE 的标识包括 IMSI (国际移动用户标识号)、TMSI (临时移动用户标识号)、P-TMSI (分组临时移动用户标识号) 以及 IMEI (国际移动设备标识号)。

通过公共信道在 UTRAN 和 UE 之间传送消息时必须用到标识号, 即在公共信道上的信令消息必须包含标识号, 这个标识号可以是永久性的或者临时性的, 临时性的标识号是在信令交换中由 UTRAN 分配给 UE 的。与用户有关的标识号是由核心网分配并存储在 USIM 当中, 可以在任何手机中使用。

在空闲模式下, UTRAN 使用 IMSI, TMSI 或

P-TMSI 来识别 UE。在连接模式下, UE 与 UTRAN 已经建立 RRC (无线资源控制) 连接, 用来传递信令。

## 2 UMTS的UE识别定位机制

### 2.1 现有UMTS技术具有改进的可行性

IMSI 是一种永久性的用户标识号, 它分别存储在 USIM 卡和 HLR (归属位置寄存器) 中, UE 第一次在网络注册时会用到 IMSI, 为了预防伪造和保护用户私密, IMSI 一般是不会在空中直接传送的。特殊情况下例外, 即网络为确定 UE 其合法性, 要求发送 IMSI, 但这不是接入网络的过程。

UE 在网络注册后, 网络分配给用户一个 TMSI 或者 P-TMSI 用于以后的信息交换, 在空中传送时, 用 TMSI 或 P-TMSI 来代替 IMSI, 可以防止伪造并且保护用户身份。在电路交换业务方面, 由 VLR (访问位置寄存器) 分配 TMSI; 在分组交换业务方面, 由 SGSN (服务 GPRS 支撑节点) 分配 P-TMSI。TMSI 只能在 VLR 的辖区内使用, 出了辖区, TMSI 就无效了。同样, P-TMSI 也只能在 SGSN 的控制区内使用, 出了控制区也就无效了。

如果 UE 与 UTRAN 第一次连接时使用 TMSI 或 P-TMSI, UE 必须提供位置区域标识号或路由区域标识号以证明它自己的身份。另外 VLR 或 SGSN 也可以在任意的时间重新分配新的 TMSI 或 P-TMSI 给 UE, 这个过程可以当成位置区域更新或路由区域更新的一部分来执行, 也可以单独执行。

在 3GPP 标准里没有定义 TMSI 和 P-TMSI 的内部结构和编码。TMSI 或 P-TMSI 长度为 32bit,

不能全为 1，最高的两个比特用来区分它是 TMSI 还是 P-TMSI，TMSI 的最高两个比特为 00、01 或 10，P-TMSI 的最高两个比特为 11，其他比特由 VLR 或 SGSN 随意指定。

2.2 改变UMTS用户识别的方法及带来的影响

为每个 UE 生成多个 IMSI，并存储在 USIM 和 HLR 中，对 IMSI 进行定期定时再分配，只有安全保密的管理层知道再分配的策略，UE 在网络中使用不同的 IMSI 注册，这需要增加已有的 USIM 和 HLR 的容量，并且修改 HLR 的部分协议。

UE 在网络中注册后，网络一次性分配给 UE 一组 TMSI 或者 P-TMSI 用于以后的通信和信令等信息交换，并且在 VLR 辖区或 SGSN 的控制区内随机的使用一组 TMSI 或者 P-TMSI 中的一个。同时，VLR 或 SGSN 也可以在任意的时间重新分配新的 TMSI 或 P-TMSI 给 UE，出了 VLR 辖区或 SGSN 的控制区，TMSI 或者 P-TMSI 就无效了，需要重新分配。这除了需要增加 VLR 和 SGSN 的容量外，还需要改变 VLR 和 SGSN 控制 TMSI 或者 P-TMSI 的协议，增加随机选择 TMSI 或者 P-TMSI 的算法。UE 与 IMSI 以及与 TMSI 或 P-TMSI 的映射关系如图 1 所示，UE 向 IMSI 是一对多映射，IMSI 向 TMSI 或 P-TMSI 也是一对多映射。

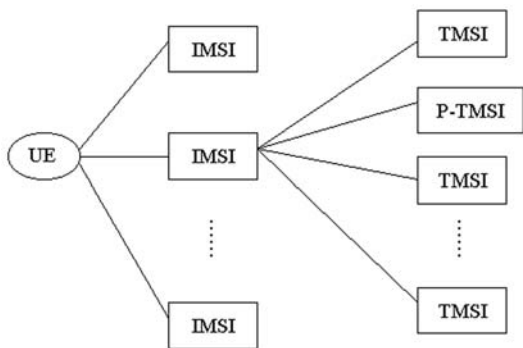


图 1 UE 与 IMSI 以及与 TMSI 或 P-TMSI 的映射关系

由于 3GPP 标准里没有定义 TMSI 和 P-TMSI 的内部结构和编码，只是规定了它们的长度，不能为全 1，以及最高两个比特的属性。所以，通过改变 VLR 和 SGSN 生成 TMSI 或 P-TMSI 的算法，

就可以改变它们的内部结构和编码，只有掌握了特定算法，才能够正确传送和接收 TMSI 或 P-TMSI，从而增加了识别和定位 UE 的难度。

上述这些措施，除了需要对 USIM 卡进行改造外，至少还需要对 CN 中的 HLR、VLR 和 SGSN 进行改造。要在工程上实现，就必须对全部 CDMA 网络的 UTRAN 进行改造，还要对 CN 进行调整，这对于一个正在运行中的商用网络来说代价太高。此外在改造过程中对设备和协议的调试，会影响现有业务的运行，极端情况可能会造成大面积 UTRAN 宕机，而造成经济损失和不良影响。

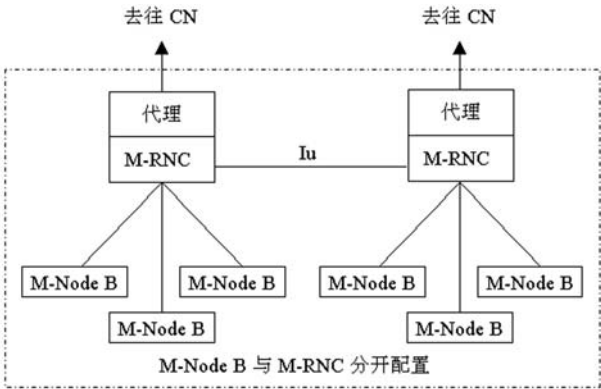
3 CDMA军用移动网络安全接入设计

UMTS 框架技术已经非常成熟，各种协议也比较完善。总体上看，协议具有很大的灵活性，为 CDMA 军用移动网络安全接入提供了可能性。由于 GSM 和 CDMA 网络已经商用，军用移动网络的安全接入协议必须与之兼容。如在全网范围内为军用移动网络的安全接入进行改造，规模巨大，成本极高，且可能因不稳定使商用网络遭受很大损失。选择建立军用子网 UTRAN，既能更好地解决军用子网用户身份的安全保密，还能够避免上述问题。

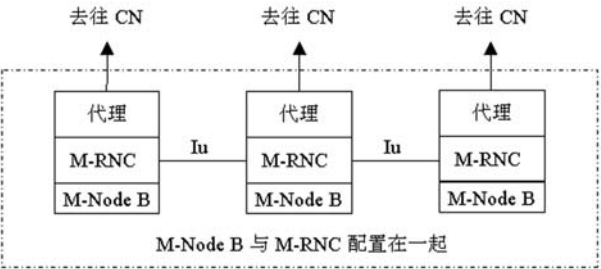
3.1 CDMA军用于网UTRAN框架

为了尽可能减少对现有 CDMA 网络的影响，我们提出军用子网 UTRAN（M-UTRAN）的概念，主要设备包括单独设计的 Node B 和无线网络控制器 RNC（M-Node B 和 M-RNC），以及用户终端。用户终端经过改造后称为 M-UE。在 M-UTRAN 中增加代理模块与 M-RNC 协同工作，完成各种映射表格和协议的转换，在军用于网和公用于网之间起到网关的作用。M-UTRAN 在应用时，M-Node B 可以与 M-RNC 分开配置，通过有线（光纤或电缆）方式连接；或者 M-Node B 与 M-RNC 配置在一起，M-UTRAN 的框架结构如图 2 所示。





(a) M-UTRAN 的框架结构



(b) M-UTRAN 的框架结构

图 2 框架结构图

3.2 军用于网内UMTS的设计思路

3.2.1 TMSI映射表设计

改造之前，TMSI 与 UE 一一对应，且保持固定不变，直到 VLR 重新分配 TMSI，识别了 TMSI 后，就可以定位 UE。在军用于网中，VLR 一次分配多个 TMSI 与 UE 对应，并且 TMSI 处于不断的变化之中。这样就增加了敌方识别 TMSI 的难度，即使识别了 TMSI，由于 TMSI 不断变化，也很难通过 TMSI 跟踪到 M-UE。多个 TMSI 存储在手机的固定或临时存储器中，修改后的映射表为一个 M-UE 对应多个 TMSI，在存储器中与 MDN（移动用户号码）的映射关系如图 3 所示，每次通信 M-UE 都随机的选择一个 TMSI 与 MDN 相对应。

3.2.2 认证鉴权机制设计

M-UE 在实际网络中所处的位置有很多种，在军用于网中，M-UE 可以与同一个军用于网的不同 M-UE 通信，也可能跨越公网与另一个军用于网的 M-UE 通信。在同一个军用于网内的呼叫直接由军用于网 UTRAN 处理；跨越公网的军用于网间通信需要经过军用于网 UTRAN 代理，经过双向认证完成鉴权，在呼叫信令离开军用于网，进入公用子网

时，分配符合公用子网的 TMSI，经过与 CN 通信完成呼叫处理后，再次从公用子网进入军用于网的时候由代理转换成符合军用于网的 TMSI。在军用于网中的 M-UE 与公用子网 UE 通信时，经过军用于网 UTRAN 代理，经过双向认证完成鉴权，在呼叫信令离开军用于网，进入公用子网时分配符合公用子网的 TMSI，之后由 CN 负责与公用子网 UTRAN 的通信。当 M-UE 处于公用子网 UTRAN 的小区中时，UTRAN 无法处理 M-UE 的认证请求，不能进行正常通信。

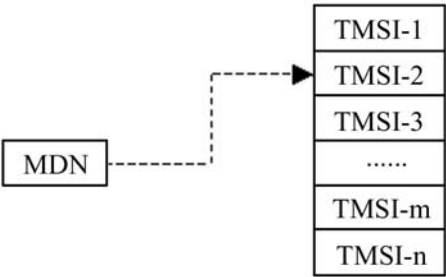


图 3 存储器中与 MDN 的映射关系

3.2.3 建立转换代理

增加代理是为了处理军用于网中 M-UE 与 TMSI 一对多的关系，在到达 CN 之前，转换成 TMSI 与公用子网 UE 一对一的关系。同时，代理还负责判断一个呼叫的目的地是军用于网还是公用子网。

3.3 应用模式

3.3.1 军民互通

CDMA 军用移动安全接入关系如图 4 所示。在军民互通的应用模式下，在正常的军用于网内部 M-UE 之间通信的基础上，军用于网的 M-UE 呼叫公用子网的 UE，并与之通信。这种模式主要用于驻军比较集中的地域，保障军队日常工作和训练中的移动通信安全接入。

3.3.2 军内互通

在军内互通的模式下，在军用于网内部 M-UE 之间通信的基础上，军用于网 M-UE 与远端军用于网的 M-UE 通信。这种模式既可用于部队运动过程的通信联络，也可以用于部队到达指定地域后，与后方基址建立通信联络。

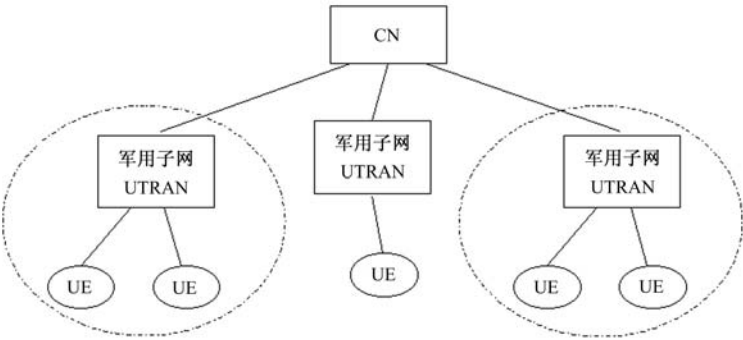


图4 CDMA 军用移动安全接入体系

4 小结

本文提出了一种在不改变 CDMA 体制下，建立军用子网 UTRAN，安全接入现有商用网络的基本方案。虽然有些具体问题，如信息加密、具体协议实现等问题尚未讨论，但是可以看出该方案在建

设和应用方面，具有系统开发相对简单、投资低、见效快、扩展性强和应用灵活等特点；在安全性上，具有用户身份隐蔽、安全控制强、军用通信隐蔽于民用通信之中等特点。应用该方案建立的军用子网 UTRAN 特别适合于秘密军事行动通信需要。

参考文献

[1] 苏信丰[美]著, UMTS 空中接口与无线工程. 朗讯科技(中国)有限公司无线工程组译. 北京: 人民邮电出版社, 2006 年 9 月第二次印刷;  
[2] 彭木根, 王文博等编著. TD-SCDMA 移动通信系统, 机械工业出版社. 北京: 2007 年 5 月第二版;  
[3] Wenbo Mao [英]著. 王继林, 伍前红等译. 现代密码学理论与实践. 北京: 电子工业出版社, 2004 年 7 月第一次印刷。

作者联系方式

通信地址: 北京丰台大成路 13 号 Y00  
邮政编码: 100039  
联系电话: 010-66820369

# 基于信号循环平稳特性的智能天线技术

张洪顺 董明山 陈磊

**摘要:** 介绍了信号的循环平稳特性, 讨论了基于信号循环平稳特性的信号源个数估计、空间谱估计及自适应波束形成, 最后给出了仿真模型和仿真结果。

**关键词:** 循环平稳特性; 智能天线; 信号源个数估计; 空间谱估计; 自适应波束形成

智能天线的主要用途有信号源个数估计技术、空间谱估计技术和自适应波束形成技术, 目前实现这些用途的算法大都是建立在信号为窄带平稳假设基础之上的, 然而这个假设并不符合所有的实际应用情况。

由于大多数的人工信号都具有循环平稳特性, 并且循环平稳信号处理技术除了具有很强的宽带信号处理能力外, 还有抗噪性能好、信号选择能力强等优点, 因此, 基于信号循环平稳特性的智能天线, 可以很好的弥补传统智能天线技术的缺点。

## 1 信号的循环平稳特性<sup>[1,2,3]</sup>

研究表明大部分人工信号如: 通信、遥测、雷达和声纳等系统中的信号都具有循环平稳特性, 它们的特定阶统计参数是随时间呈周期性变化的, 这类信号统称为“循环平稳信号”(cyclostationary signal)。如果信号  $x(t)$  的均值  $mx(t)$  和自相关函数  $R_{xx}(t, \tau)$  具有以下性质则可以定义  $x(t)$  为循环平稳信号。

$$mx(t) = mx(t+T) \quad (1)$$

$$R_{xx}(t, \tau) = R_{xx}(t+T, \tau) \quad (2)$$

$T = k/\alpha$ ,  $k$  为整数,  $\alpha$  为循环频率,  $R_{xx}(t, \tau)$  的定义式如下

$$R_{xx}(t, \tau) = E[x(t+\tau/2)x^*(t-\tau/2)] = R_{xx}(t+k/\alpha, \tau) \quad (3)$$

式中\*表复共轭,  $x(t)$  的循环相关函数  $R_{xx}^\alpha(\tau)$  为自相关函数  $R_{xx}(t, \tau)$  的傅立叶变换

$$R_{xx}^\alpha(\tau) = F[R_{xx}(t, \tau)] = \left\langle x(t+\frac{\tau}{2})x^*(t-\frac{\tau}{2})e^{-j2\pi\alpha t} \right\rangle \quad (4)$$

$\langle \bullet \rangle$  表示对全部时间取平均,  $R_{xx}^\alpha(\tau)$  的傅立叶变化即为循环谱密度函数

$$S_{xx}^\alpha(f) = \int_{-\infty}^{\infty} R_{xx}^\alpha(\tau) e^{-j2\pi f\tau} d\tau \quad (5)$$

如果一个过程  $x(t)$  的循环自相关函数  $R_{xx}^\alpha(\tau)$  对所有非零  $\alpha$  及延迟参数不恒等于零, 则此过程在时域内具有循环频率为  $\alpha$  的循环平稳特性, 而在频域呈现出在频偏  $\alpha$  处的谱相关性。对于平稳过程(如平稳噪声)不具有循环平稳性, 其  $R_{xx}^\alpha(\tau)$  对所有非零  $\alpha$  值恒等于零, 即当  $\alpha \neq 0$  时, 谱相关函数  $S_{xx}^\alpha(f)$  等于零, 因此循环平稳信号处理具有很强的抗噪能力。

一般来讲信号的循环频率  $\alpha$  和信号的调制方式以及载频、基带码元速率等参数有关, 不同的信号往往具有不同的循环频率族  $\{\alpha\}$ 。通过适应的选取循环频率可以从多重信号中提取出感兴趣的信号, 而抑制其他的信号的影响, 即实现信号的可选择性。

## 2 阵列信道模型

设智能天线共  $M$  个阵元, 各阵元以间距  $D$  排列成均匀线阵, 以阵列的第一个阵元为参考阵元; 设共有  $d$  个互不循环相关的远场源信号, 相应入射角分别为  $\theta_1$ 、 $\theta_2$ 、...、 $\theta_d$ ; 参考阵元接收到的  $d$  个源信号分别表示为  $s_1(t)$ 、 $s_2(t)$ 、...、 $s_d(t)$ , 且  $s_k(t)$  ( $k=1, \dots, d$ ) 是循环平稳信号, 对应的循环频率为  $\alpha_1$ 、 $\alpha_2$ 、...、 $\alpha_d$ ; 智能天线阵列的感应信号向量可表示成为:

$$X(t) = [x_1(t), x_2(t), \dots, x_M(t)]^T \quad (6)$$

$(\bullet)^T$  为转置运算; 其中, 向量  $X(t)$  中第  $i$  个元素为  $x_i(t)$  可表示成:

$$x_i(t) = \sum_{k=1}^d s_k [t + (i-1)D \sin(\theta_k)/c] + n_i(t) \quad (7)$$

注意式(7)没有对源信号的带宽做出任何要求。

### 3 信号源数估计

信号源个数估计是空间谱估计的基础,只有是在信号源个数估计正确的情况下才能进行有效的空间谱估计。已有的信号源个数估计方法如盖氏圆方法<sup>[4,5]</sup>、EGMs<sup>[6]</sup>、BEM<sup>[7]</sup>等都是建立在窄带信号的假设之上的,而基于信号循环平稳特性的信号源个数估计算法既适用于窄带信号也适用于宽带信号。

以阵列的第1阵元为参考阵元构造循环互相关向量

$$R_{1X}^\alpha(\tau) = [R_{11}^\alpha(\tau), R_{12}^\alpha(\tau), \dots, R_{1M}^\alpha(\tau)]^T \quad (8)$$

构造伪数据矩阵如下

$$R_{1X}^\alpha(NT) = \begin{bmatrix} R_{11}^\alpha(0), & R_{11}^\alpha(T), & \dots, & R_{11}^\alpha(NT) \\ R_{12}^\alpha(0), & R_{12}^\alpha(T), & \dots, & R_{12}^\alpha(NT) \\ \vdots & \vdots & & \vdots \\ R_{1M}^\alpha(0), & R_{1M}^\alpha(T), & \dots, & R_{1M}^\alpha(NT) \end{bmatrix} \quad (9)$$

$T$ 是采样间隔,  $NT$ 是最大时延,于是可得循环互相关向量  $R_{X1}^\alpha(\tau)$  的协方差矩阵  $C = R^\alpha(NT)(R^\alpha(NT))^H$ ,  $(\bullet)^H$ 表示共轭转置,对  $C$  进行特征值分解,假设在  $d$  个源信号中对于循环频率  $\alpha$  只有  $d_\alpha$  个源信号存在非零循环自相关函数。可得

$$C = \sum_{k=1}^{d_\alpha} \lambda_k e_k e_k^H + \sum_{i=d_\alpha+1}^M \sigma_n^2 e_i e_i^H \quad (10)$$

由上式可知对协方差矩阵  $C$  用文献[6]给出的EGMs算法就能较为准确的估计出具有循环频率为  $\alpha$  的信号源个数。

### 4 空间谱估计

最早利用信号循环平稳特性进行空间谱估计的算法是由W.A.Gardner教授提出的Cyclic MUSIC和Cyclic ESPRIT<sup>[8]</sup>但是这些方法都是基于窄带信号假设之上的。在此基础之上Xu等人提出了即适用于窄带信号也适用于宽带信号的SC-SSF(spectral correlation method based on signal

subspace fitting)方法<sup>[9]</sup>。为了简单起见,在此延续上一节的讨论,如果对于循环频率  $\alpha$  只有  $d_\alpha$  个源信号存在谱相关特性,由文献[2]可知式(9)可以化为

$$R_{1i}^\alpha(\tau) = \sum_{k=1}^{d_\alpha} r_{s_k}^\alpha [\tau + (i-1)D \sin(\theta_k)/c] e^{j\pi\alpha(i-1)D \sin(\theta_k)/c} \quad (11)$$

因此  $R_{X1}^\alpha(\tau)$  又可以写成如下矩阵形式

$$R_{X1}^\alpha(\tau) = \sum_{k=1}^{d_\alpha} A(\alpha, \theta_k) R_{s_k}^\alpha(\tau) \quad (12)$$

式中

$$R_{s_k}^\alpha(\tau) = [r_{s_k}^\alpha(\tau), r_{s_k}^\alpha(\tau + D \sin(\theta_k)/c), \dots, r_{s_k}^\alpha(\tau + (M-1)D \sin(\theta_k)/c)]^T$$

$$A(\alpha, \theta_k) = \text{diag}(1, e^{j\pi\alpha D \sin(\theta_k)/c}, \dots, e^{j\pi\alpha(M-1)D \sin(\theta_k)/c})$$

与传统的MUSIC算法一致,由  $e_{d_\alpha+1}, e_{d_\alpha+2}, \dots, e_M$  张成的空间为噪声空间,它与信号空间正交,因此,对  $R_{X1}^\alpha(\tau)$  的协方差矩阵  $C$  运用传统的MUSIC算法可以估计出具有循环频率  $\alpha$  的信号的来波方向,更换循环频率,重新构造协方差矩阵  $C$  再进行运算,直到将所有信号的来波方向都估计出来为止,显然,该算法不受信号源个数必须少于阵元个数的限制。

### 5 自适应波束形成

传统的波束形成有基于信号波达方向(DOA)的波束形成与基于用户传输训练序列的波束形成。前者需要估计波达方向或信号的导向矢量(阵列流形),并且对阵列流形的校验要求非常高,而后者需要在传送的信号中加入训练序列,接收端首先要对训练序列进行同步,然后利用训练序列来训练阵列的权矢量<sup>[10]</sup>。为了克服这些问题近年来人们提出了很多盲波束形成的算法,它们大致可以分为三类:①常模量算法,利用信号的常模量特性提取有用信号,但它不能保证权值收敛到全局最优。②基于高阶累积量算法,利用信号高阶统计量的特性,去除高斯噪声,但是对于非高斯信号处理起来就比较困难了,并且该算法运算复杂、收敛速度慢。③基于信号循环平稳特性算法,由于几乎所有的通信信号都具有循环平稳性,并且很容易找出它们之间不同的循环频率,相比之下该算法具有明

显的优势,是当前国际上研究的热点,其新算法层出不穷,在此只介绍性能较为稳定的一种 ECAB (Eigenspace-based Cyclic Adaptive Beamforming) 算法。

吴强等人根据信号的循环平稳特性提出了 CAB<sup>[11]</sup>类算法,其代价函数为

$$\begin{cases} \max |w^H \hat{R}_{xu} c| \\ w^H w = c^H c = 1 \end{cases} \quad (13)$$

式中  $\hat{R}_{xu} = \overline{[X(n)U^H(n)]_N}$  表示  $N$  次采样的平均值,  $X(n)$  为  $X(t)$  的数字采样,  $U(n) = X^*(n+\tau)e^{j2\pi\alpha n}$ , 上标共轭符号“\*”当且仅当使用共轭自相关特性时才使用,相应的迭代快速算法为

$$w_{CAB} = \frac{n-1}{n} w_{CAB}(n-1) + \frac{1}{n} \sum_{m=1}^M U_m^*(n) X(n) \quad (14)$$

式中  $U_m(n)$  表示矢量  $U(n)$  的第  $m$  个元素。该算法收敛速度快,但是没有考虑噪声抑制问题,不能在干扰方向形成零陷,因而在强干扰情况下无法工作。为此吴强等人将线性约束最小方差 (LCMV) 波束形成技术与 CAB 算法结合提出了约束周期自适应波束形成 (Constrained CAB, C-CAB) 算法,其权值表达式如下

$$w_{C-CAB} = \hat{R}^{-1} w_{CAB} \quad (15)$$

式中  $\hat{R} = \overline{[X(n)X^H(n)]_N}$ , 该算法在性能上大优于 CAB 算法,但收敛速度慢且在低信干比情况下性能仍受到影响。接下来我们讨论利用空间约束来提高它的性能,将式 (15) 写成如下形式:

$$w_{C-CAB} = (E_s \Lambda_s^{-1} E_s^H + E_n \Lambda_n^{-1} E_n^H) w_{CAB} \quad (16)$$

由文献 [11] 可知  $w_{CAB} \rightarrow \alpha(\theta)$ , 因此,

$E_n^H w_{CAB} = 0$ , 所以 (16) 式可以写成

$$w_{C-CAB} = E_s \Lambda_s^{-1} E_s^H w_{CAB} \quad (17)$$

显然权值矢量  $w_{C-CAB}$  收敛于信号子空间内,然而由于快拍次数的限制及 CAB 算法估计出来的导引矢量的误差,所以算法的性能必定受到来自噪声子空间分量的影响而大下降。如果我们直接将信号导引矢量的估计值  $w_{CAB}$  投影到信号子空间

$$w_p = \hat{E}_s \hat{E}_s^H w_{CAB} \quad (18)$$

用新的权矢量代替 (15) 式中的  $w_{CAB}$ , 从而得到了新的波束形成算法,即 E-CAB 算法。(18) 式的投影带来两个好处:一是将估计的导引矢量约束在信号子空间内;二是降低了有限次快拍相关阵所引起的子空间扰动的影响,提高输出信噪比,加快了算法的收敛速度。

## 6 计算机仿真

### 6.1 仿真模型

以 8 元均匀直线阵为例,假设空间有 3 个远场调幅信号  $s_1$ 、 $s_2$ 、 $s_3$ , 它们的载波分别为  $f_1$ 、 $f_2$ 、 $f_3$ , 其中  $f_1 = f_3 = 1.1 * f_2$ , 相对带宽均为 40%, 信噪比为 3dB, 信干比为 0dB, 来波方向分别为  $-20^\circ$ 、 $40^\circ$ 、 $10^\circ$ , SC-SSF 算法采用的循环频率  $\alpha = 2f_1$ , E-CAB 算法以  $s_2$  为有用信号, 采用的循环频率为  $\alpha' = 2f_2$ , 建立如下仿真模型。

Simulation Model of Smart Antenna Based on Cyclostationarity

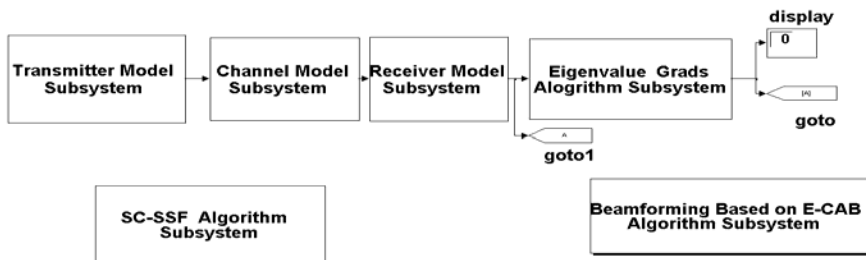


图1 仿真模型

6.2 仿真结果及分析

当仿真稳定以后，图 2 中的 display 模块的显示结果一直稳定在 2，图 3 中的两个谱峰也一直稳定在  $-20^{\circ}$  和  $10^{\circ}$  的两个位置上只是峰值有轻微的变

化，在  $40^{\circ}$  方向上没有出现谱峰，由此可以看出该算法具有很好的信号选择能力，从图 4 可以看出 E-CAB 算法在  $40^{\circ}$  方向上形成最高增益的谱峰。

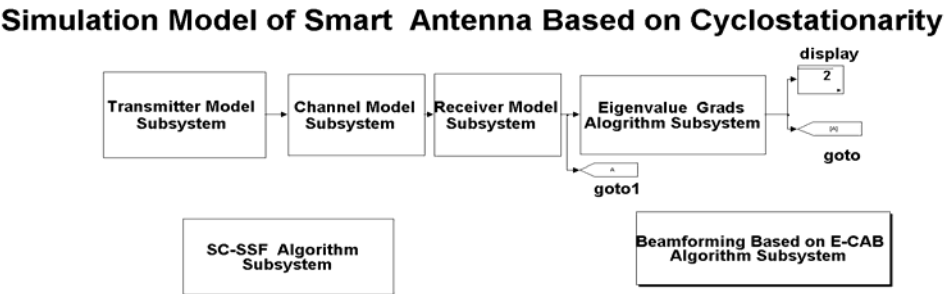


图 2 信号源个数估计结果

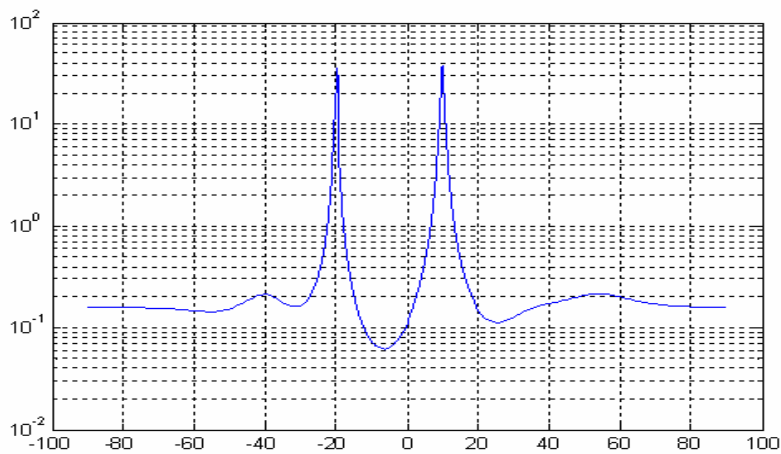


图 3 利用 SC-SSF 算法空间谱估计结果

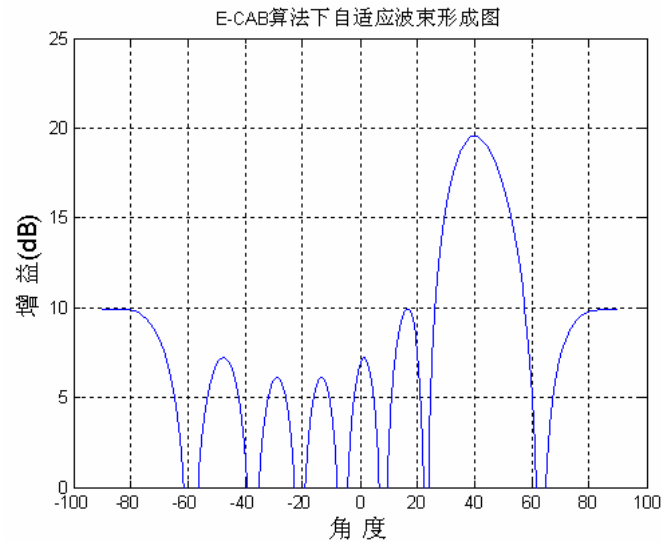


图 4 以  $s_2$  有用信号的自适应波束形成结果

## 7 结束语

通过将信号的循环平稳特性引入到智能天线中,较好的实现智能天线的空间信号源个数估计、空间谱估计及盲自适应波束形成。与传统的智能天

线技术相比,该方法不仅适用于窄带信号也适应于宽带信号,同时还提高了智能天线的抗噪能力和信号选择能力。

### 参考文献

- [1] 黄知涛,周一宇,姜文利.循环平稳信号处理与应用[M].北京:科学出版社,2006.
- [2] 范达,李晔,张莉,吴瑛.利用信号循环平稳性提高谱估计测向性能[J].信息工程大学报,2003(1):27-31.
- [3] 金梁,姚敏立,殷勤业.宽带循环平稳信号的二维空间谱估计[J].通信学报,2000(3):7-11.
- [4] 刘鸣,袁超伟,贾宁,黄韬.智能天线技术与应用[M].北京:机械工业出版社,2007.
- [5] H. T. Wu, J. F. Yang and F. K. Chen, Source Number Estimator Using Gerschgorin Disks, proc ICASSP, Adelaide, Australia, pp261-264, Apr.1994.
- [6] Jingqing Luo, Zhiguo Zhan. Using Eigenvalue Grads Method to Estimate the Number of Signal Source, proc.ICASSP2000, pp223-225.
- [7] JIANG Lei, CAI Ping, YANG Juan, WANG Yi-ling, XU Dan. A New Source Number Estimation Method Based on the Beam Eigenvalue[J].Journal of Marine Science and Application. Vol.6.No.1.March 2007, pp.41-46.
- [8] Gardner W.A.Simplification of MUSIC and ESPRIT by exploitation of cyclostationarity. Proc.IEEE, 1988, 76(7):845-847.
- [9] Xu G. H, Kailath T. Direction-of-arrival estimation via exploitation of cyclostationarity-a combination of temoral and spatial processing. IEEE Trans. Signal Processing, 1992, 40(7):1775-1785.
- [10] 张发启,张斌,张喜斌.盲信号处理及应用[M].西安:西安电子科技大学出版社,2006.
- [11] Wu Q, Wong K M. Blind adaptive beamforming for cyclostationary signals.IEEE Trans on sp, 1996.44(1):2757-2767.

### 作者联系方式

通信地址:重庆通信学院

邮政编码:400035

联系电话:13228689859

# 复杂光电环境下激光末制导炮弹作战效能评估方法

张立 周丰平

**摘要:** 本文采用系统分析 SEA 方法,对战场复杂光电干扰环境中的激光末制导炮弹作战效能进行较全面的分析,并建立了动态效能评估模型,为在光电对抗条件下科学评估激光末制导炮弹作战效能提供了一条有效的途径。

**关键词:** 激光末制导; 光电干扰; 效能评估

## 1 引言

武器系统的作战效能是指在一定的环境条件下,系统完成规定作战任务的程度。纯静的理想作战环境是不存在,复杂光电环境是信息化战场主要特征。在充斥光电干扰的复杂作战环境中,准确地评估激光末制导武器的作战效能,就需要分析光电干扰对激光末制导武器作战效能的影响。

## 2 系统、环境与使命的确定

SEA 方法(system effectiveness analysis)基于六个基本概念:系统、使命、环境、原始参数、性能量度和系统效能。

激光末制导武器系统主要由激光指示器、执行同步器、观察所电台、阵地电台、指挥同步器、末制导武器等部分组成。

**环境:** 独立于系统之外部分,主要有作战地域的地形;敌方兵力组成等。

**使命的确定**同系统运行环境及作战战术背景密不可分,其主要依据是战术想定。想定:

1) 兰方一坦克群(T 辆)成横队队形,以时速  $V_m$ ,向红方防御前沿发动进攻。

2) 红方运用激光末制导武器系统攻击距前沿 5000m 内敌坦克。

3) 地形为平原,天气晴,白天。

4) 兰方对红方进行激光压制性干扰和通信干扰,以确保坦克群成功突破。

5) 红方激光末制导武器系统的作战使命是将兰方坦克消灭或阻击在一定距离之外(如敌坦克有效直射程  $D_E$  之外)。

红方末制导武器系统的性能可用二个性能量度来刻画:一个是平均击毁敌坦克数(DTN),用以度量总的武器系统阻止威胁数目的能力;另一个为射击成功率(FSP),即命中弹占总发射弹的比例,从总体上评价武器系统命中概率。

所选系统参数组的  $\{X_i\}$  每一组值代表系统的一个状态,通过建立映射关系得到一组  $\{DTN, FSP\}$  值,当原始参数在其值域内变动时,效能空间就形成系统轨迹  $L_s$ 。

在该情况下,红方使命要求被简单表述为在一定的防御距离外( $D_E$ ),至少击毁敌一定坦克数( $\lambda$ ),以确保整个防御战斗的胜利。系统效能通过对比系统轨迹和使命轨迹和相对几何关系,得出效能和具体测度值(MOPs)。设  $V(L)$  是轨迹  $L$  上的一种测度,则:

$$E = \frac{V(L_s \cap L_m)}{V(L_s)}$$

式中:  $L_s$  为系统轨迹;  $L_m$  为使命轨迹。

## 3 系统映射的建立

### 3.1 地形环境

(1) 发现目标精确位置的概率

激光末制导武器系统对运动目标射击时,观测站必须发现并能目视目标。观察员使用光学仪器发现并认清运动坦克的概率为:  $P_0$

$$P_0 = 1 - 2 \int_0^x \frac{1}{\sqrt{2\pi}\sigma_D} e^{-\frac{(x-D)^2}{2\sigma_D^2}} dx$$

式中:  $D$  表示目观距离,  $\sigma_D^2$  表示观察距离的散布方差。  $\sigma_D^2$  值可按  $D$  值查表求得。



## (2) 暴露行驶距离和通视性分析

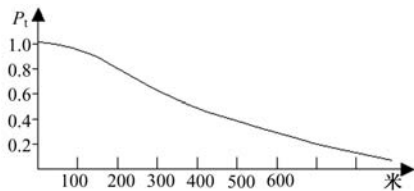
激光末制导武器属于人工制导武器，只有当观察者从发现、测定、计算、口令传送、发射弹体、制导激光照射目标直到命中这段时间区间内，目标完全连续通视，才能保证射弹命中目标。在此时间内，目标暴露行驶的距离称为有效暴露行驶距离  $d_m$ ，用下式描述：

$$d_m = V_m \left( t_s + \frac{D_{PM} - V_m \times t_s}{V_f + V_m} \right)$$

式中： $V_m$  为目标运动速度； $t_s$  为观察者从发现目标至武器飞抵目标所需时间，即完成一次攻击所需时间； $D_{PM}$  为武器发射地至目标距离； $V_f$  为末制导武器飞行速度。

对观察者而言，受地形因素的影响，目标暴露行驶距离长短完全是随机现象。故可用目标暴露行驶距离分布函数描述，其过程如下：

首先在作战地域电子地图上确定观察点和观察照射界，在此视界内按一定等分角  $\theta$  作观察轴线，而后采用离散判定法计算各轴线上等间隔点的通视性（间隔为  $\Delta L$ ），根据轴线上各等间隔点的通视性及各点的相邻关系，可知轴线上不同连续通视距离的分布状况。统计各轴上不同连续通视距离分布状况，可绘出连续暴露距离分布函数  $P_l$ 。上述过程计算量很大，可通过编程计算。下图为某平原地区的量化分析结果：



## 3.2 激光压制性干扰环境

在激光压制性干扰环境下，影响激光末制导武器命中目标的主要因素有：激光照射误差、制导误差以及兰方激光干扰器的压制性干扰。

激光照射误差：由照射目标形成光斑（直径  $R$ ）所引起，服从圆内均匀分布，分布大小与红方激光器至坦克距离  $D_{GM}$  有关：

$$R = 500 \times D_{GM} \sin(0.4 \times 10^{-3})$$

制导误差：服从正态分布，其方向和距离误差相等，都为  $E_m$ ；接收信号迟延误差：射弹接受的激光反射信号是脉冲信号，间隔为  $\tau_1$ ，而目标作连续运动  $V_m$ 。因而引起偏差  $V_m \tau_1$ 。若目标毁伤幅员

为  $2l_x \times 2l_z$ ，将激光照射误差看作系统误差，制导误差看作单独误差，通过合并计算，则在无干扰条件下的命中概率  $P_D$ ：

$$P_D = \int_{-l_x}^{l_x} \int_{-l_z}^{l_z} \frac{\rho^2}{\pi E_m} e^{-\rho^2 \left[ \frac{(x_m - V_m \tau_1 \cos \gamma)^2 + (z_m - V_m \tau_1 \sin \gamma)^2}{E_m^2} \right]} dx_m dz_m$$

$$\text{其中: } E_m = \sqrt{E_m^2 + 0.125 \times \left( \frac{\pi}{4} R^2 \right)}$$

压制性干扰：兰方的随队激光干扰武器对末制导武器导引部进行干扰，使末制导弹体丢失目标。其成功率同末制导武器导引部接收到的信干比有关。末制导武器导引部接收到干扰激光功率  $P_{cj}$  为：

$$P_{cj} = \frac{P_j \tau_{aj} \tau_c S_r}{R_j^2 \phi}$$

式中： $P_j$ 、 $\phi$  分别为激光干扰武器发射功率和发散立体角； $R_j$  为激光干扰武器与末制导弹体的距离； $\tau_{aj} = e^{-aR_j}$  为干扰武器与末制导弹体之间的大气透过率，其中  $a$  为大气消光指数； $\tau_c$ 、 $S_r$  分别为弹体导引部的透过率和在干扰方向上有效接收面积。而此时，弹体导引部接收到的引导信号功率（即坦克反射激光功率） $P_{cs}$  为：

$$P_{cs} = \frac{\rho \tau_t \tau_c S_c}{\pi} * \frac{P_s \tau_{as} \cos \alpha \cos \beta}{R_t^2}$$

式中： $\rho$  为坦克表面对光的反射系数； $\tau_t$ 、 $P_s$  分别为红方激光器光的透过率和发射功率； $\tau_c$ 、 $S_c$  分别为弹体导引部的透过率和有效接收面积； $R_t$  为坦克到末制导弹体的距离；大气透过率  $\tau_{as} = e^{-a(R_t + L)}$ ，其中  $L$  为红方激光器至坦克的距离。角  $\alpha$  为坦克在弹体导引部方向上的仰角； $\beta$  为坦克至末制导弹体与坦克至红方激光器之间在水平面上投影的夹角。

则在压制干扰下，进入弹体导引部的引导信号与干扰信号功率之比，即信干比用  $K$  表示：

$$K = \frac{P_{cs}}{P_{cj}}$$

当信干比小于某一临界系数  $K^*$  时，兰方干扰成功率  $P_g = 1$ ，否则失败  $P_g = 0$ 。

## 3.3 电子干扰环境

红方处于兰方坦克射程之外时，兰方另一主要对抗手段是电子干扰红方指挥通信系统，达成软杀

伤，使红方激光末制导武器无法正常工作。在图 2 给出通信指挥系统在敌电子干扰下运行状态图。

图中每一步  $P$  均为电子干扰条件下完成各项工作概率， $1-P$  为该步截止概率，所以系统运行状态正常的概率为各步完成概率的连乘形式。根据试验资料表明，因坦克车体装甲和屏蔽作用，使得部分命中末制导武器失效，以  $k$  表示命中弹毁伤坦克概率，则在通视条件下，1 枚激光末制导武器毁伤坦克概率  $P_{DTN}$ ：

$$P_{DTN} = kP_0P_tP_D(1-P_g)P_{cd}P_{js}P_{tx}P_{fs}P_{tb}P_{ts}P_{zs}P_{mz}$$

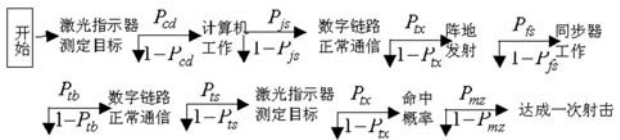


图 2 通信指挥运行状态图

4 系统轨迹

通过以上分析，系统性能量度（DTN，FSP）都能导出。设  $P_{DTNi}$  第  $i$  次射击毁伤坦克的概率，则

$$\begin{cases} DTN = \sum_{i=1}^N P_{DTNi} \\ FSP = \frac{DTN}{N} \\ N = \frac{5000 - D_E}{V_m \times t_s} \end{cases}$$

5 使命轨迹

实战中，激光末制导武器主要同其他反坦克武器结合使用。合理配置构成远、中、近多层反坦克火网。在该情况下，红方任务要求可简单表述为在一定的防御距离之外，至少击毁敌坦克  $\lambda$  辆，确保整个防御战斗的胜利。这样任务的客观性减少到单一要求 DTN，其使命轨迹在性能空间内的区域必须满足不等式：

$$\lambda \leq DTN$$

比较系统轨迹和使命轨迹空间的关系，可得出系统的效能（MOE）。

6 模拟模型

上述解析模型参数多，解析式过于复杂，且某些参数在交战过程中完全是随机的，如坦克航路角总是在一定范围内变化的，难以确定，但这却恰恰适合 Monle-carlo 方法求解的特点，因而本文建立模拟模型，运用计算机仿真求解。模型计算程序流程图见图 3。

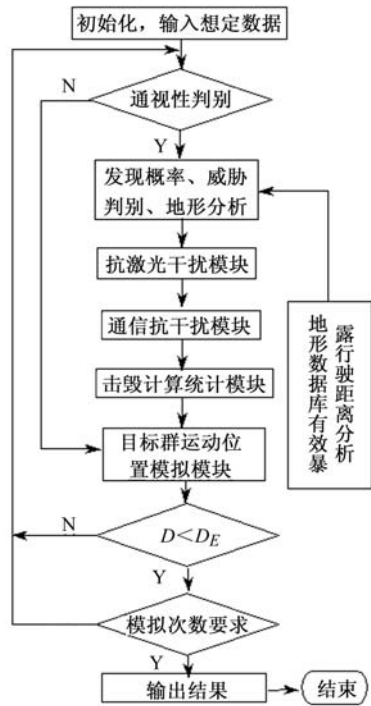


图 3 计算程序流程框图

按仿真模型框图编制仿真软件，输入不同的战术方案运行软件，可以从不同角度分析系统效能。本文主要进行了以下几方面的效能分析：

- 1) 典型战情条件下，武器系统按战术原则配置情况下的效能计算分析。
- 2) 武器系统的极限地理环境分析。对于特定任务要求下，通过变化地形通视率距离分布概率因素，计算其对系统效能的影响，从而寻找系统效能趋于零的环境作为系统的极限地理环境。
- 3) 武器系统效能的敏感度分析。通过光电干扰的性能参数值的变化对系统效能的影响分析，找到系统效能对其最为敏感的因素。
- 4) 武器系统承受任务能力。

## 7 结束语

SEA 方法框架结构是由德辛和莱维斯提出的,首先应用于评估  $C^3I$  大型系统。本文运用 SEA 方法分析激光末制导武器系统是一次尝试,在充分考

虑现代信息作战“大环境”因素的影响,构建模型具有一定的“柔性”(Flexible),对光电干扰、地形等因素的变化敏感,因而模型具有较强的适应性和可扩展性的特点。

### 参考文献

- [1] 邵国培等. 电子对抗作战效能分析[M]. 北京: 解放军出版社, 1998.
- [2] 李志良等. 军事地形分析与利用[M]. 北京: 八一出版社, 1993.

### 作者联系方式

通信地址: 重庆通信学院军事教研室

邮政编码: 400035

联系电话: 023-68760804 15902366923

# 体系结构设计方法对军队信息化建设的影响

张永红 左琳琳 赵利平 席欢

**摘 要:** 规范的体系结构设计已成为顶层设计不可缺少的重要内容。目前,以美英为代表的外军正在逐步形成并完善体系结构设计方法,使其在外军信息化建设中发挥着日益重要的作用。本文介绍了美国和英国体系结构设计方法的主要内容,并简要分析了体系结构设计方法对外军信息化建设的影响。

**关键词:** 体系结构; 设计; 信息化建设

## 1 体系结构设计方法的发展变化

美军最早开始规范 C4ISR 的体系结构设计,其主要目的是解决作战需求的描述方法不统一,研制的系统功能不能很好满足作战需求,不同系统缺乏统一的技术标准和规范等问题。1995 年,在美国当时的副国防部长指示下,在前 C3I 助理国防部长的亲自领导下,美军于 1996 年 10 月、1997 年 12 月发布了《C4ISR 体系结构框架》1.0、2.0 版,将其作用 C4ISR 系统体系结构设计规范。

随着新军事变革向深入发展,信息化水平日益提高,信息系统已渗透到装备领域和业务领域的各个方面,迫切需要在进行武器装备体系和业务系统的顶层设计时,就能保证各类装备和业务系统的无缝信息交联。武器系统的发展,不再孤立于体系之外,而要从满足构建一体化武器装备体系的高度,统筹考虑它的规模、数量和能力,以及与其他武器系统的信息交联,从而保证信息化武器装备体系中,各类武器装备配比合理、协调配合。美军多年的实践经验表明,《C4ISR 体系结构框架》建立的体系结构设计方法,是实现上述目标的有效手段。2004 年 2 月,发布《国防部体系结构框架》(DODAF) 1.0 版,将应用范围从 C4ISR 系统扩展到国防部各个任务领域。2007 年 4 月,美军又发布了 DODAF1.5 版,今后还将不断进行完善,为美军提供更为科学、实用的顶层设计方法。

世界主要国家纷纷研究、借鉴美军的体系结构设计方法。英国于 2005 年 8 月 31 日发布了《英国国防部体系结构框架》1.0 版(简称 MODAF1.0)、2007 年发布了 1.1 版,北约也发布了《北约体系结构框架》及《北约 C3 技术体系结构》。

## 2 美国体系结构设计方法的核心内容

目前,美国国防部主要采用视图方法进行体系结构设计。所谓“视图”,是指描述事物的角度,就是从不同角度,描述对系统的要求。这好比在机械制图中,需要俯视图、顶视图和侧视图描述对一种机械零件的要求一样。DODAF 规定,在设计一种体系的体系结构时,要从总体、作战、系统与服务、技术标准的角度描述。每一种视图由若干文档、表格或图形组成,即“产品”或“视图产品”。DODAF1.5 版共确定了 29 种产品,其中包括 2 种全视图产品、9 种作战视图产品、16 种系统与服务视图产品和 2 种技术标准视图产品。在开发某一体系结构时,可根据具体需要开发其中的若干产品。产品描述的内容如表 1 所示。

### 2.1 作战视图及产品

作战视图用于描述系统所支持的任务和活动(既包括作战任务,也包括业务活动)、作战要素和节点、节点间相互关系,以及完成或支援作战所要求的信息流。它规定了信息交换的类型、交换频率、信息交换支持何种任务与行动。其核心内容是清楚、完整地描述军事行动参与者的关系和信息需求。利用作战视图,可以检查业务流程是否合理、各项条令政策是否可行;可以确定作战需求,如通信流量、节点之间互操作等级、安全保密要求等,并根据作战需求做出资源配置和系统发展决策。

表 1 《国防部队系统结构框架》1.5 版中的视图产品

视图产品	名称	主要内容
AV-1	概述与摘要信息	描述体系结构的范围、用途、用户、环境描述、分析结果，以及版本信息
AV-2	综合词典	给出该体系结构中所有术语的定义
OV-1	高级作战概念图	用图形/文本对作战概念进行描述，形象说明该体系结构所支持的作战使命、任务、作战节点及连接关系等
OV-2	作战节点连接描述	描述作战节点及其连接关系，以及各节点之间的信息交换需求
OV-3	作战信息交换矩阵	描述各作战节点之间需要交换的信息及信息属性，如传输媒介、质量和互操作等级等
OV-4	组织关系图	描述该体系结构中的组织、角色及其之间的指挥关系
OV-5	作战活动模型	描述该体系结构涉及的各种能力、作战活动以及之间的关系
OV-6a	作战规则模型	描述作战或业务活动遵循的规则
OV-6b	作战状态转换描述	描述作战活动的动态关系，包括作战活动发生的时间特性、顺序特性等
OV-6c	作战事件追踪描述	描述作战场景下或重要作战系列事件中作战活动的轨迹
OV-7	逻辑数据模型	描述作战视图的系统数据需求以及业务规则
SV-1	系统接口描述	描述系统节点、节点内的系统，以及在节点内和节点间系统之间的连接关系
SV-2	系统通信描述	描述系统节点、系统部件之间的通信链路或网络配置
SV-3	系统相关矩阵	描述各种系统之间的关系
SV-4a	系统功能描述	描述系统不同层次的功能，以及各种系统功能之间的数据流
SV-4b	服务功能描述	描述服务所实现的功能，以及各种服务功能之间的服务数据流
SV-5	作战活动与系统功能的映射矩阵	描述作战活动与系统功能的映射关系
SV-5b	作战活动与系统的映射矩阵	描述能力与作战活动、作战活动与系统功能、系统功能与系统映射关系，从而得到能力与系统的映射关系
SV-5c	作战活动到服务的映射矩阵	描述服务与作战活动的映射关系
SV-6	系统数据交换矩阵	描述系统之间交换的系统数据元素的详细情况，以及这些交换数据的属性
SV-7	系统性能参数矩阵	详细说明系统及其硬件、软件、接口、功能的现有性能参数，以及在未来特定时期的性能参数
SV-8	系统发展描述	描述更新某个已有系统或者开发某个新系统以满足未来需求的步骤
SV-9	系统技术预测	预测在给定期限可能使用并将影响体系结构未来发展的新技术和硬、软件产品
SV-10a	系统规则模型	描述由于系统设计或实施原因对系统功能的约束
SV-10b	系统状态转换描述	描述某个系统对改变其状态的不同事件所做出的响应
SV-10c	系统事件跟踪描述	确定作战视图中关键事件序列所需要的系统具体功能
+SV-11	物理模型	定义各种类型的系统数据结构。如，消息格式、文件结构、物理模型
TV-1	技术标准配置	所有系统视图产品应采用的标准
TV-2	技术标准预测	描述特定时间范围内新出现的技术标准及其对系统视图产品的潜在影响

2.2 系统与服务视图及产品

系统与服务视图用于描述满足上述作战要求的系统的组成单元、功能和系统组成单元之间的相互关系等。其内容不仅包括多个系统如何链接和互操作，也可以描述单个系统的关键硬件和软件，各部件的连接关系、电路和网络，所在的位置，以及具体系统和部件的性能参数等。系统视图必须能把支持作战活动、作战节点间信息交换的系统资源与作战视图进行关联，并进一步细化对作战视图中描述

的信息交换属性，把作战视图中节点之间的信息交换转化为系统视图中系统之间的通信容量要求、安全保护要求等。系统视图产品可用于以下目的：制定投资决策，以高效费比的方式满足作战要求；评估和改进互操作能力。

2.3 技术标准视图及产品

技术标准视图是决定系统组成要素的组织、相互关系的一组最低限度的规则，主要包括一组技术标准、惯例、规范和准则。制定技术标准视图的目

的是提供制定工程规范、建造通用模块、开发产品生产线所依据的技术实施指南。采用技术标准视图，可以提高效率、改善互操作性，确保开发人员对技术发展进行充分的计划。

2.4 全视图产品

全视图产品描述的是与整个体系结构有关的信息，主要为体系结构的范围和背景。其中，范围包括体系结构涉及的内容和时间跨度；背景则包括与体系结构有关的条令、战术技术与程序、相关目标和构想表述、作战概念、作战想定以及外部环境条件等。

另外，最终形成体系结构产品要依靠体系结构的工具即相关软件来完成。美军为了提高体系结构的设计水平，降低设计成本，积极鼓励采用商用体系结构工具。此外，美军还十分重视用于描述建立

体系结构信息的逻辑数据模型等通用参考资源的建设，用于存储供体系结构设计用的体系结构数据、产品的体系结构知识库的建设，以提高体系结构设计的开发效率和水平。

3 英国体系结构设计方法的核心内容

MODAF 参考 DODAF，也采用了“视图”和“产品”概念对体系结构进行描述。MODAF 共定义了 6 类视图（如图 1 所示）、38 种视图产品，其中包括新增了 6 个战略视图产品和 2 个采办视图产品，并对作战视图、系统视图和技术视图作了 6 处修改，在用户手册中规定了必须强制采用的 15 种视图产品。

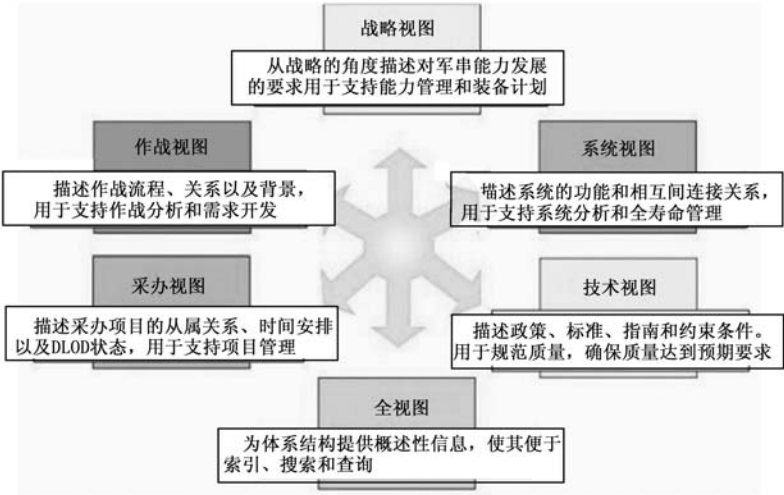


图 1 MODAF 视图

3.1 战略视图

战略视图（StVs）从战略角度描述对军事能力的发展要求。其实现过程是：按能力分类法将相关政策 and 概念细分为各种能力。通过战略视图确定了

各种军事能力的从属关系，明确了所要开发的能力。战略视图主要由政策/概念分析领域的人员以及一类用户开发和使用。

表 2 战略视图产品

StV-1	能力构想	描述了特定时间段内某一能力的构想
StV-2	能力分类	列表表示某些能力及某一特定时期、某一能力领域所需要的各种子能力（称为能力功能）
StV-3	能力阶段划分	不同时间段拟获得的能力
StV-4	能力群	提供分析各种能力之间主要关系的方法
StV-5	能力与系统部署的对应关系	通过“系统”、“装备”、“训练”等与机构/时间段的相互关系，表示某种能力的部署状况
StV-6	能力功能与作战的对应关系	描述各能力要素与作战活动之间的对应关系，以及能力分析 with 作战活动分析之间的关系

3.2 作战视图

作战视图（OVs）用于描述完成英国防部各项使命所需的任务与行动、作战节点与要素以及之间的信息交换需求。作战视图可用于开发用户需求、

形成未来作战方案、支持作战计划的制定等。在英国防部采办周期内，一些投资者将开发和使用权作战视图。例如，二类用户将利用作战视图支持用户需求报告的拟制和完成作战计划的制定。

表 3 作战视图产品

OV-1a	高级作战概念图	描述高级作战概念的图形/文本
OV-1b	作战概念描述	补充描述高级作战概念图
OV-1c	作战性能属性	提供了与高级作战概念图中的想定/应用案例有关的作战性能属性细节
OV-2	作战节点连接描述	描述了作战节点、连接关系，以及各节点之间的信息交换需求
OV-3	作战信息交换矩阵	描述了各节点之间的信息交换，以及这些交换的相关属性
OV-4	组织关系图	描述组织、任务或组织间的其他关系
OV-5	作战活动模型	描述了能力、作战活动、作战活动输入、输出之间的关系；相关的覆盖图可给出费用、节点或其他相关信息
OV-6a	作战规则模型	描述了约束作战活动的作业规则
OV-6b	作战状态转换描述	描述了应对事件的作业流程
OV-6c	作战事件轨迹描述	追踪某个想定或一系列事件中踪迹的行动
OV-7	逻辑数据模型	作战描述系统数据要求及结构化的业务流程规则

3.3 系统视图

系统视图（SVs）描述支持国防部作战和业务功能的系统（主要是通信和信息系统，但不限于此）及其互连关系。系统视图用于将系统资源与作

战视图关联起来，主要用途之一是开发满足用户需求的系统方案，并由此提出合理的系统需求。系统视图将主要由英国防部采办部门及其供应商开发与使用。

表 4 系统视图产品

SV-1	系统接口描述	描述了系统节点、系统、系统项目，以及节点内和节点间的相互连接
SV-2a	系统端口规范	描述系统端口，以及同其他系统通信时端口使用的协议
SV-2b	系统与系统的端口连接	描述两个端口连接时使用的协议栈
SV-2c	系统连接群	描述系统端口之间的单一连接和按组进行的节点间的逻辑连接
SV-3	系统关系矩阵	描述给定体系结构中系统间的关系；或描述系统类型接口、以及计划中的与现有接口间的关系等
SV-4	系统功能描述	描述系统的功能，以及系统各功能间的数据流
SV-5	作战活动与系统功能间映射矩阵	描述系统与能力的关系，或系统功能与作战活动的关系
SV-6	系统数据交换矩阵	详细描述系统之间交换的系统数据要素，以及这些数据交换的特征
SV-7	系统性能参数矩阵	描述一定时间范围内系统视图要素的性能特征
SV-8	系统发展描述	描述将一批系统改造成为更有效系统，或致力于现有系统发展的实施步骤
SV-9	系统技术预测	给定时间内预计可得到的和将影响未来体系结构发展的新兴技术及软硬件产品
SV-10a	系统规则模型	描述系统设计或执行中由于某些原因对系统功能的约束
SV-10b	系统状态转换描述	描述系统对事件的响应
SV-10c	系统事件轨迹描述	对作战视图中一系列关键事件进行细致系统描述
SV-11	物理图示	描述逻辑数据模型实体，如消息格式、文件结构、物理图解等的物理实现

### 3.4 技术视图

技术视图 (TVs) 是一组表格, 包含适用于体系结构的标准、规则、政策和指南。虽然称为技术视图, 但内容并不完全是技术方面的, 它既包括各

种系统（如各种标准和协议），也包括各种作战行动（条令、标准使用程序和战术技术程序）。主要由一体化产品小组中负责标准化的官员在采办寿命周期内进一步细化和管理工作。

表 5 技术视图产品

TV-1	技术标准轮廓	列举某一给定体系结构中所有视图产品采用的标准
TV-2	技术标准预测	描述特定时间内，新技术标准及其对给定体系结构所有视图产品的潜在影响

### 3.5 采办视图

采办视图用于描述计划的细节，包括项目的从属关系和“国防发展序列”（DLODs）中的军事能力集成关系。通过这些视图，可以确定项目与计划

之间的相互影响，整合各种采办活动。采办视图为负责能力管理与采办的人员提供重要的计划信息，可用于确认某一交付的综合军事能力的成熟度。

表 6 采办视图产品

AcV-1	大系统采办群	详细描述采办任务如何分组，以提高互操作性管理和项目管理
AcV-2	大系统采办规划	描述整个采办计划或一组子计划的概貌

### 3.6 全视图

全视图 (AVs) 是体系结构的顶层描述, 包括体系结构的适用范围、所有者、时间跨度, 以及为

有效搜索和查询体系结构模型所需的其他元数据。全视图提供了未来访问和利用体系结构模型所需的关键信息, 因此都是必需的。

表7 全视图产品

AV-1	概述及摘要信息	包括范围、用途、用户、环境描述、分析结果以及有关体系结构的版本信息
AV-2	综合词典	定义了体系结构所用要素的分类法

#### 4 体系结构设计方法对信息化建设的主要影响

构建信息化武器装备体系是一项规模庞大的系统工程。以美军为主导的这种规范的体系结构设计方法,能够清晰描述复杂武器系统所支持的作战任务和作战能力需求,确定系统的功能、组成结构及其关系、采用的技术标准等。不同系统的体系结构集成在一起,就成为描述满足各种作战任务需求的武器装备体系的蓝图。因此,体系结构方法已在战略谋划、需求论证、采办管理、提高武器装备互操作性等方面发挥日益重要的作用。概括起来其作用

主要包括:

一是在战略谋划方面,借助体系结构设计,将联合作战概念转变为信息化装备体系建设的宏观需求。二是在装备体系规划方面,借助体系结构设计,分析重复建设、需要发展的新的系统。三是在采办管理方面,借助体系结构设计,不断细化作战需求、系统功能与技术标准。四是在系统设计方面,借助体系结构设计,加强系统用户方与开发方的沟通。五是在实现武器装备一体化方面,借助体系结构设计,保证异构系统的互操作。

参考文献 (略)

## 作者联系方式

通信地址：中国国防科技信息中心      邮政编码：100036      联系电话：010-66357093



# 基于策略的军事综合网络管理系统研究

朱巍 单维峰 易慧

**摘 要:** 本文主要介绍了一种军事网络管理系统的模型, 这种模型是基于动态策略的网络管理系统, 它提供了一种自动化的方法来动态配置和管理网络设备, 最后, 本文根据模型进行了系统试验, 结果证实该模型实时有效、功能强大并且具有很好的扩展性。

**关键词:** 网络管理; 基于策略; 策略协商

## 1 概述

在新一代的网络管理技术中, 基于策略的网络管理已经成为最有发展前景的网管技术。基于策略的网络管理方法(PBNM)消除了以设备为中心的传统方法常常引发的许多网络配置差错, 大大提高了管理效率和可伸缩性, 并使网络工作者把工作的重点放在业务需求而不是设备配置的细节上, 从而提高了管理的抽象化程度。

目前, 现有的军事通信网一般是由许多独立管理的专业技术网系互联组成的, 它们大多采用各自的管理协议, 互不兼容, 这样导致了即使是一个网系中的通信网中也有多个不同管理功能和服务设施的子网管理系统的共存。而大部分的基于策略的解决方案都是基于单厂商的, 不同的厂商策略的互不兼容使通信网管理系统更加复杂, 通信管理人员不得不通过不同的管理域管理每一个子网, 对于网络业务提供者(SP)来说, 管理系统最好通过一个策略控制平台就可实现对所有管理域的信息监视、配置管理和安全交互。针对上述问题, 未来的基于策略的军事综合网络管理系统必须具有以下的特点: 最高授权人可以通过策略管理网内的所有资源, 从高级到低级, 直至端系统; 通过对用户级别的评估提供相应的服务和安全级别; 保证策略文件和策略协商的机密性、真实性和完整性; 对策略文件提供长期的存储以备查询和恢复; 对于相关域的策略协商不需要通过集中的方式由策略制定人或上级领导进行协调仲裁; 可以对网络设备的状态进行动态的配置。

本文主要提供了一个基于策略的军事网络管理系统 PBMNM (policy-based military network management) 的范例, 可广泛使用于建立和管理军

事通信网络, 尤其是可以迅速的部署和配置一个综合环境下的安全网络, 同时, 该系统也可以被用于管理控制这些安全网络, 这个基于策略的综合处理方案可以运用于安全性、自动化程度比较高的信息化战场环境中。

## 2 PBMNM的体系结构

基于策略的网络管理的基本目标是使用户在较高的层面上表示、配置信息, 或提供配置管理的模板, 网络管理员不必了解设备的具体细节就可完成对设备的配置管理, 从而大大简化了网络的配置和管理。PBMNM 的网络管理体系结构由以下核心组件构成: 策略控制台, 它是网络管理人员定义和编辑策略的一种管理工具; 策略决策点(PDP), 它的功能包括策略检索, 策略翻译, 策略冲突检查, 接收来自策略执行点的策略请求以及返回策略给策略执行点; 策略库(PR), 这是用来保存策略的目录服务器; 策略编辑器(PE), 主要用于调整和编辑策略文件; 策略协商代理(PNP), 它是用来为策略决策点处理策略协商对话的, 它是整个系统与远程域唯一直接通信的模块; 策略执行点(PEP), 它通过访问列表, 队列管理算法和其他方式执行策略的网络设备, 如被策略激活的交换机或路由器等。

如图 1 所示, 在该系统的结构中, 所有的 PBMNM 组成除了 PNP 以外的部分都被假定在安全的网络环境中, 不能直接和外部的系统通信。与远程 PNP 模块通信的 PNP 设备位于一个屏蔽局域网中, 在军事局域网的保护范围之外, 但是仍然在防火墙中。图 1 中所有的示例域中都包含 4 个 PEP 设备: 防火墙、一个 VPN 设备、路由器和一个

DNS 控制设备。防火墙和 VPN 的 PEP 设备都是位于防火墙设备之中，VPN 的 PEP 设备建立和保持 IPSEC 通道来进行远程通信，防火墙 PEP 设备用于执行协商服务信道规则，路由器 PEP 设备为远程网络保持路由通道在本地域中，并且判定服务质量参数，DNS 服务器为本地域的服务器对远程域的

服务器分配姓名绑定。PDP 和策略库通信使用 HTTP 协议和 XPATH 查询语言，和 PEP 的通信使用 COPS 的扩展协议 COPS-PR。策略编辑器和策略控制台使用 SSL/TLS 协议来保证通信的安全。PDP 和 PNP 通信和 PNP 内部通信一样都是使用 SSL/TLS 协议进行通信。

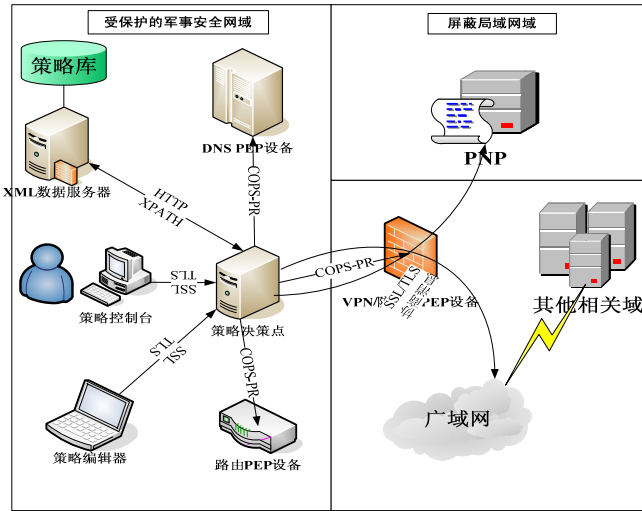


图 1 系统的体系结构

策略使用扩展标记语言（XML）表示，但是系统体系结构与策略文档独立无关，这样可以导致一个高扩展性的系统以支持各种不同类型的策略而不用对结构作任何调整。然而，一部分策略仍然会有其特殊性的地方，在系统构成中必须考虑到这一点，所以在 PDP 中会包含一个软件组成模块叫策略处理单元（PPU）。一个完全独立的策略处理单元必须对 PBMNM 系统中的每一种相应的策略都能作出处理。

### 3 系统设计

#### 3.1 策略的制定和管理

授权最高的用户可以通过策略编辑器来创建和修改策略文件，在编辑的过程中，用户通过和 PDP 通信，并从用户的公共核心验证信息获取相应级别的安全信道进行通信。当一个策略文件已经编辑好了，策略编辑器会申请用户的数字签名并且递交策略文档给 PDP 并且在携带一个策略类型验证，PDP 获得验证然后递交文档给相关联的 PPU 进行处理。PPU 会确认策略文档中的数字签名，验证策略文档是符合正确的 XML 语法结构，核实文档相关

联的策略说明。在确认策略文档是可信的、经授权的和有效的之后，PPU 为文档添加一个特别的标识符，并且添加 PDP 的数字签名以保存用户的原始信息，然后将策略文档保存进策略库中。当策略文档中包含一个新的远程域的策略时，PPU 开始和远程域进行协商。如果策略文件对一个已经存在远程连接的策略进行改变时，PPU 会和那个远程域进行重新协商。如果策略文件对一个已经存在的远程连接遗漏了一个策略时，PPU 会撤销该先前创建的远程连接。在所有的例子中，PPU 控制所有的最终设备配置结果。

#### 3.2 动态策略协商

策略的协商过程包含四种策略协商对象：策略建议对象、协商抄本对象、策略恢复对象和策略撤销对象。所有的策略协商对象都包含一种策略类型、一种策略对象类型、一个特别的标识符和有效时间、PDP 认可该对象的数字签名。数字签名也包含有自己单独的标识符和有效时间来保护以对抗假扮使用和重复使用等攻击。

一旦一条策略被创建或者升级，PPU 会对应的对策略的每一个远程域的校验创建出一条策略建议对象。PPU 通过对远程域发出一条策略建议对象开

始协商序列，一个远程的 PPU 会通过发出一条协商抄本对象来回应它，协商抄本对象就是所接受的策略建议对象的复制加上一个声明回应，这个声明包含反应的状态（接受，拒绝或者无法判断）和相应的理由。建议评估后的结果会位于协商抄本对象的最上面详细说明。当 PPU 发出一个可接受的协商抄本对象并且从远程域收到一条可接受的协商抄本对象就意味着一次策略协商成功完成了。每一次

PPU 成功完成一次策略协商之后都要发出一条策略恢复对象。当一个协商完全完成时，每一个 PPU 会将本地的协商抄本对象和远程的协商抄本对象的信息联合起来产生一个合并的策略文件，双方的 PDP 都可以执行。每一个 PPU 然后按照协商后的策略对相应的 PEP 设备进行配置。最后，每个 PPU 周期性发出一条策略恢复对象来表示协商策略仍然有效。

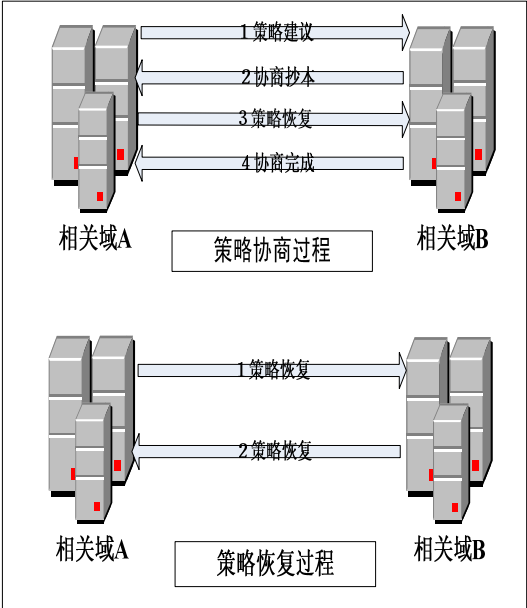


图2 动态策略协商

策略恢复对象同样可以使用在重建先前的协商策略，这样就不需要进行整个全部的协商序列了，这一般发生在连接丢失、网路断线或者 PDP 系统的崩溃之后的恢复。所有本地和远程产生的策略协商对象都会作为样本存放在本地的策略库中以便审查和快速重建协商策略，在存入策略库之前，本地的 PDP 对接受的策略协商对象签上数字标签。

所有涉及远程域的本地策略库中的策略协商对象都有策略文件中的一个详细的实例相关联，这样 PDP 可以很容易的从当前的策略文档回溯到最近的策略建议对象，再到回应的协商抄本对象和策略恢复对象，最终找回整个策略协商目标。当 PDP 被激活时，它首先为这条存在的策略协商对象的过程检查策略库，如果这个过程存在，PDP 就会试图去重新创建这之前的协商策略，它会发布一条策略恢复对象而不会进行整个全部的协商序列。它为 PDP 系统的中断提供了一个迅速快捷的恢复途径。

```
Global policy scope..
MainPreamble..
{..
CoaPreamble. CoaPreamble {}..
Local policy controls {}..
Remote policy controls {}..
}..
Coalition policy scope..
CoaPreamble..
{..
Declarations {}..
Local policy controls {}..
Remote policy controls {}..
}..
Service access rules..
{..
Local service requirements {}..
Local service provisions {}..
}..
AD policy scope..
AD Preamble..
{..
Declarations {}..
Local policy controls {}..
Remote policy controls {}..
}..
Service access rules..
{..
Local service requirements {}..
Local service provisions {}..
}..
}
```

图3 合并协商策略格式

3.3 策略协商代理

PNP 是用来为 PDP 处理策略协商对话的，它是整个系统与远程域唯一直接通信的模块。它对每一个远程的 PNP 设备建立一个安全鉴别通信通道，同时使用公匙证书来进行协商。本地的 PNP 会校验远程的 PNP 是否得到远程域的授权。PDP 通过一条专门的双向安全鉴别信道使用控制消息指导 PNP 和远程域协商。这些控制消息可以指导 PNP 为每一个特殊类型的策略配置详细的远程 PNP 或者为一个远程的 PNP 去掉某个类型的策略。本地的 PNP 发出状态消息给本地的 PDP 来证实远程 PNP 系统连接信道的有效性。在 PNP 之间传输策略协商对象的消息报头包含足够的信息可以对不同种类的策略在策略协商中的多元化技术，并且对不同种类的策略允许独立的协商序列。

与 PDP 不同，PNP 说明策略协商对象的具体内容，同时也不包含协商的状态。它只是仅仅由本

地 PDP 控制传输策略协商对象,就如同一个不透明的载体一样。而且,PNP 不能影响协商,虽然所有的策略协商对象通过 PDP 发送。PDP 使用合并后的策略文件来产生低级别的策略以适用于对 PEP 设备的配置管理,并使用 COPS-PR 协议对 PEP 设备提供这些配置策略。当一个 PEP 设备被激活,它首先和它的初始的 PDP 使用先前配置的网络地址建立一个 COPS 会话,在一个 COPS 的配置请求中告知 PDP 设备的性能,PDP 回应提供其所有与 PEP 设备相关的策略。PEP 设备保持与 PDP 的 COPS 会话使得 PDP 可以当相关策略改变时随时发送策略改变的消息。PEP 设备也同时可以在任何时候报告性能的改变和状态给 PDP。最终,稳定的

COPS 会话可以使得所有的设备在某些设备重启和出故障时更敏感和快捷。

4 系统的实现

本系统的作用环境主要是在非安全的广域网中的可靠军事网络域,系统是基于分布式结构下的,包含策略的制定和动态策略的提供。策略的准备促进综合化网络的快速使用,动态策略的提供使得网络设备(防火墙、私人虚拟网络连接、路由、服务质量和域名服务等)的配置和管理更加自动化。具体的系统模型如图 4 所示。

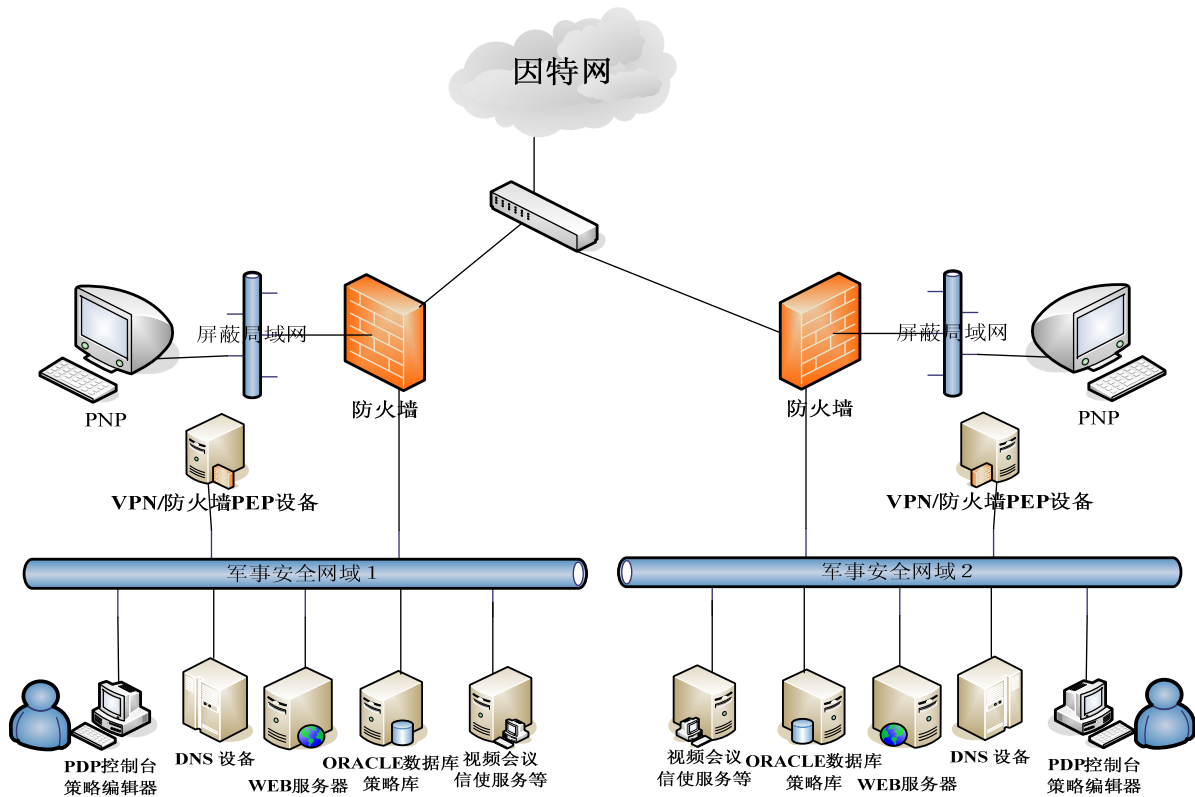


图 4 系统模型实现

PBMNM 的全部组件: PDP、PNP、策略编辑器、策略控制台全部都是用 JAVA 实现,本文选择了在 J2EE (Java 2 Platform, Enterprise Edition) 平台上编译执行。策略编辑器和策略控制台都是使用图形用户界面,便于人机交互。各个操作平台都是基于 windows xp 操作系统的。如图四所示,系统的环境由两个不同的域组成,外部通过因特网进行互相连接,每个控制域包括一个 VPN 防火墙设备,一个用户工作站和一组本地控制域服务,如网

点,数据库和能够通过网络连接向远程控制域提供的视频终端。

在两个域中,所有 PBMNM 组件的平台是 Intel Pentium 4 3.2 GHz processors with 3 GB RAM running Microsoft Windows Professional, SP2。实现的验证主要通过策略来配置网络连接,以及一个策略的改变是怎样产生一个网络重新配置来适应条件的改变和对系统的性能的影响。

试验结果表明:在建立与单个远程控制域的网

络连接时,策略的提交和确认的时间大大缩短了;当一个策略发生变化,可以在30秒内进行重新协商,完整的配置会在五分钟之内完成;当系统发生问题需要策略恢复时,策略恢复机制会在短时间内恢复原有的策略配置。综上所述,除去一些在调试中出现的次要问题,模型系统的安全性、稳定性和自动化程度都有着很大的提高。

## 5 结束语

本文提出了一种基于策略的军事综合网络管理

系统的结构,并对其性质和技术进行了介绍和说明。并且根据系统模型设计了系统实践。虽然在策略的编辑、高级别策略的支持和对外部事件的自动化处理方面还有很多不足,但是,模型系统的能力比较之前的系统自动化程度更高,安全性更好,并具备更好的扩展性。综上所述,系统的实现验证了动态策略的协商和提供对快速部署和管理军事网络的效果和意义。

## 参考文献

- [1] Zhu Wei: Research on an Integrated Network Management System. Eighth ACIS International Conference on SoftwareEngineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, page 311-336, July 2007
- [2] UMU-PBNM, University of Murcia Policy-Based NetworkManagement, <http://pbnm.dif.um.es/>
- [3] ITU-T. Recommendation X.701 - Systems Management Overview, Aug. 1997.
- [4] L. Gong. JXTA: A Network Programming Environment.5 (3) :88-95, 2001.
- [5] G. Goldzmidt and Y. Yemini. Distributed Management by Delegation. 15th Int'l. Conf. Distrib. Comp. Sys., pages 333-340, May/June 1995.
- [6] Web-based Enterprise Management (WBEM), <http://www.dmtf.org/standards/wbem/>.
- [7] S.Rabie. Object-Oriented Network Operations for Packet Switching Networks, Proceedings of IEEE Network Operations and Management Symposium, NOMS 1992.
- [8] 夏海涛,詹志强. 新一代网络管理技术[M]. 北京:北京邮电大学出版社, 2002.1
- [9] 王厚生,郭詮水. 军事通信网网络管理. 北京:军事科学出版社, 2002.2

## 作者联系方式

通信地址:武汉市解放公园路45号通信指挥学院20队

邮政编码:430010

联系电话:13277900070

# 基于仿真测试的信息融合能力评估技术研究

邹伟 刘伟

**摘 要：**本文首先总结了舰载信息融合系统现行评估指标存在的缺陷，然后从作战使用的角度，提出了海战场舰艇信息融合固有能力概念，并描述了该固有能力的四个指标。最后给出了在实验室仿真测试条件下，计算固有能力指标的算法。  
**关键词：**仿真测试；信息融合；指标；评估

## 1 前言

多种海上试验结果显示，在实验室测得的正确相关率很高的融合系统，常常表现出令人难以接受的融合性能。例如两部雷达观测的同一批目标，经融合系统处理后仍会保留两个目标，尽管这两个目标看上去相隔很近。

分析融合系统出错的原因有很多，但一个很重要的事实是，这些融合系统在实验室测试中都显示很高正确相关率，常常是 95%~100%。为什么正确相关率很高的融合系统在实际应用环境下会出现简单条件都融合不上的情况呢？

根据信息融合相关的定义，相关就是“建立某时刻传感器的输出数据和其他传感器输出数据的关系，以确定这些输出数据是否来自同一个目标的处理过程”。如果来自同一个目标，就认为是正确相关，否则就是错误相关。按照正确相关的定义，上面例子中出现两个目标时，其正确相关率仍然是 100%。可见，正确相关率指标不能正确反映融合系统的实际性能。

对于航迹融合来说，融合的过程可以分为空间配准，时间配准、相关和航迹合成等，相关只是融合算法的一部分内容，正确相关率只能反映融合性能的某一个方面。但是融合的最终目的是将不同传感器输出的信息形成统一态势，纠正传感器输出信息中的错误，提高统一态势的精度。因此从相关性方面评判融合系统的性能天生就有局限性。

另外，对某些融合相关算法来说，正确相关率并不合适。例如“全邻”类算法认为每个落入相关区域内的点迹都有可能源于真实目标，只是每一个点迹与真实目标的关联概率不同，如果用正确相关率指标，只有来自于真实目标的点才是正确目标，

其余全是错误的。显然正确相关率指标就不能反映“全邻”类算法的真实内涵，这种评估就失去了意义。

在实际应用中，对指挥员来说，融合态势是否如实地反映真实态势是最重要的，正确相关率的高低没有指导意义。融合态势中有多少目标是可以相信的，有多少是重复的或者虚假的，所使用的融合系统又会以多大的概率遗漏掉实际存在的目标，这些都是信息融合系统能力问题。我们认为信息融合能力是信息融合系统的一种固有属性，它不随评估手段的改变而改变，在给定的信息源条件下，当融合算法确定后，融合系统所具有的融合能力也就确定了。因此寻找一种客观的方法来揭示这种能力就是本文的目的。

## 2 仿真测试评估系统原理

评估的依据是融合系统输出的样本数据。获取融合输出样本并最大限度提高样本数量的方法就是建立信息融合仿真测试系统。通过编制覆盖各种有效等价类和边界条件的测试用例，测试信息融合系统的能力。一个经实践检验运行稳定的信息融合仿真测试评估系统原理图如图 1。

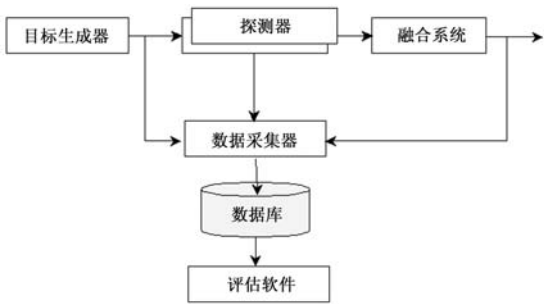


图 1 信息融合仿真测试评估系统原理图



如图 1, 测试评估系统主要由五部分组成, 分别是目标生成器、探测器、数据采集器、数据库和评估软件。融合系统是被评估对象。

目标生成器的主要功能是读进测试想定文件, 按照想定文件设定的态势和控制逻辑进行模拟运行, 产生真值目标。产生的目标情报数据通过网络发送给探测器和数据采集系统。

探测器可以是各种雷达、声纳等传感器。探测器的主要功能是接收目标生成器产生的真值目标情报, 按照探测器的探测模型发现目标, 生成探测目标列表, 并根据想定文件的控制在探测目标上叠加误差, 再将带误差的目标情报发送给融合系统。同时探测目标也发送给数据采集系统。

数据采集器的主要功能是接收各个系统产生的数据并存储到数据库。它接收目标生成器产生的真值目标数据, 接收探测器产生的探测目标情报数据, 接收融合系统输出的融合目标情报数据。同时, 数据采集系统也监视各个数据通道的状态, 向目标生成器提供数据存储完毕信号。

数据库的主要功能是存储测试数据。

评估软件的主要功能是对存储在数据库中的样本数据按照信息融合能力指标进行评估。

### 3 信息融合能力评估指标与算法

#### 3.1 概念与符号系统

针对图 1 给出的信息融合测试评估系统, 可以得到图 2 所示的评估原理图。

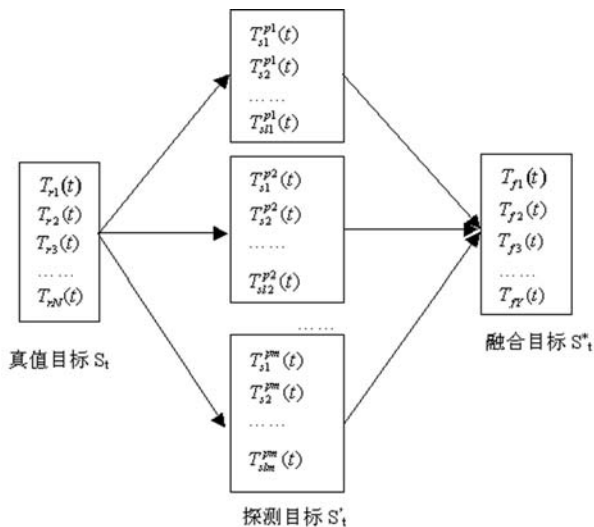


图 2 评估原理图

如图对应仿真测试系统的目标生成器、探测器和融合系统的输出, 分别有真值目标  $S_t$ 、探测目标  $S_t^d$  和融合目标  $S_t^*$ 。

设某次实验室仿真测试起止时刻为  $t_b$  和  $t_e$ ,  $t(t_b \leq t \leq t_e)$  时刻的真实态势  $S_t = [T_{r1}(t), T_{r2}(t), \dots, T_{rN}(t)]^T$  由  $N$  个真值目标组成, 这  $N$  个目标被  $M$  个来自不同平台的探测器  $\{P_1, P_2, \dots, P_M\}$  探测到, 探测器  $P_m$  探测的  $X_m$  个目标为  $S_t^{p_m} = [T_{s1}^{p_m}(t), T_{s2}^{p_m}(t), \dots, T_{sM}^{p_m}(t)]^T$ 。融合系统根据这  $P$  个传感器的输出融合成  $Y$  个融合目标航迹, 融合系统的输出即融合态势记为  $S_t^* = [T_{f1}(t), T_{f2}(t), \dots, T_{fN}(t)]^T$ 。考虑融合态势  $S_t^*$ , 虽然理论上力求与真实态势  $S_t$  一致, 但实际由于技术原因, 还不能百分之百保证一致。分析  $S_t^*$  目标与  $S_t$  真值目标的对应关系, 有以下几种情况:

1) 对于给定的融合态势  $S_t^*$  中的融合目标  $T_{fi}(t)$ , 在真实态势  $S_t$  中可以找到一个真值目标  $T_{rj}(t)$ ,  $T_{fi}(t)$  与  $T_{rj}(t)$  的状态参数在给定的评判准则下可以认为是一致的, 则  $T_{fi}(t)$  是  $T_{rj}(t)$  的像,  $T_{rj}(t)$  是  $T_{fi}(t)$  的源。  $T_{fi}(t)$  所给出的航迹称为正确航迹。

2) 对于给定的融合态势  $S_t^*$  中的融合目标  $T_{fi}(t)$ , 在真实态势  $S_t$  中找不到一个真值目标  $T_{rj}(t)$ , 使得  $T_{fi}(t)$  与  $T_{rj}(t)$  状态参数在给定的评判准则下可以认为是一致, 则  $T_{fi}(t)$  是一个虚假目标。

3) 真实态势  $S_t$  中的真值目标在传感器输出态势  $S_t^d$  中有象存在, 但未在融合态势  $S_t^*$  中出现。这种情况表示融合系统发生了目标丢失, 称为漏情。

在第 1) 种情况中, 有两个融合目标  $T_{fi}(t)$  与  $T_{fj}(t)$  ( $i \neq j$ ) 在  $S_t$  中可以找到同一个源  $T_{rk}(t)$ , 则  $T_{fi}(t)$  与  $T_{fj}(t)$  是重复目标。

重复目标和虚假目标构成了融合态势中的错误航迹。

### 3.2 信息融合能力指标

信息融合能力指标就是要反映图 2 给出的融合态势中正确航迹、错误航迹和漏情目标的比例，为此引入正确航迹率、重复航迹率、虚假航迹率和漏情率指标。

#### (1) 正确航迹率

正确航迹率就是融合态势中正确航迹占融合态势航迹总数的比例。

设  $t$  时刻，融合态势  $S_t$  中正确航迹的数目为  $Qdc(t)$ ，航迹总数为  $Qd(t)$ ，融合态势在  $t$  时刻的正确航迹率  $\rho_{dc}(t)$  为：

$$\rho_{dc}(t) = \frac{Qdc(t)}{Qd(t)}$$

由于某个时刻的正确航迹率具有偶然性，不能代表整个生命周期内航迹的正确性，不同算法也不能简单通过一个时刻的正确航迹率来判断好和差，因此在实际评估时需要引入一个能够反映全生命周期航迹正确性的指标：平均正确航迹率。

在  $[t_b, t_e]$  时间段内，平均正确航迹率定义为：

$$\rho_{dc} = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \rho_{dc}(t) dt = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \frac{Qdc(t)}{Qd(t)} dt$$

#### (2) 重复航迹率

重复航迹率就是融合态势中重复的融合目标占融合态势目标总数的比例。

设  $t$  时刻，融合态势  $S_t = [T_{r1}(t), T_{r2}(t), \dots, T_{rN}(t)]^T$  中的目标个数为  $Qd(t)$ ，重复目标数为  $Qr(t)$ ，融合态势  $t$  时刻的重复航迹率  $\rho_r(t)$  为：

$$\rho_r(t) = \frac{Qr(t)}{Qd(t)}$$

与平均正确航迹率类似，在实际评估时需要引入一个能够反映全生命周期航迹重复性的指标：平均重复航迹率。在  $[t_b, t_e]$  时间段内，平均重复航迹率定义为：

$$\rho_r(t) = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \rho_r(t) dt = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \frac{Qr(t)}{Qd(t)} dt$$

#### (3) 虚假航迹率

虚假航迹率就是融合态势中找不到真值源的融合目标占融合态势目标总数的比例。

设  $t$  时刻，融合态势  $S_t = [T_{r1}(t), T_{r2}(t), \dots, T_{rN}(t)]^T$  中的目标个数为  $Qd(t)$ ，虚假目标数为  $Qp(t)$ ，融合态势  $t$  时刻的虚假航迹率  $\rho_p(t)$  为：

$$\rho_p(t) = \frac{Qp(t)}{Qd(t)}$$

与平均正确航迹率类似，在实际评估时需要引入一个能够反映全生命周期航迹虚假性的指标：平均虚假航迹率。在  $[t_b, t_e]$  时间段内，平均虚假航迹率定义为：

$$\rho_p(t) = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \rho_p(t) dt = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \frac{Qp(t)}{Qd(t)} dt$$

#### (4) 漏情率

漏情率就是真值目标范围内所有传感器探测到的真值目标未被融合系统表示的比例。

设  $t$  时刻，被探测到的真值目标个数为  $Ql(t)$ ，融合态势中，这些真值目标未被发现的个数为  $Ql(t)$ ，则  $t$  时刻融合系统的漏情率  $\rho_l(t)$  为：

$$\rho_l(t) = \frac{Ql(t)}{Q(t)}$$

在  $[t_b, t_e]$  时间段内，平均漏情率定义为：

$$\rho_l = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \rho_l(t) dt = \frac{1}{t_e - t_b} \int_{t_b}^{t_e} \frac{Ql(t)}{Q(t)} dt$$

### 3.3 评估算法

在实际评估时，上述指标的计算必须离散化。由于仿真测试系统是数字仿真，可以比较方便地获取样本的离散量。

设  $\Delta t$  为样本采样间隔， $t_i, i = b, b+1, \dots, e$  为采用时刻， $Qdc(t_i)$ 、 $Qd(t_i)$  分别为该时刻融合态势的正确航迹数和航迹总数。则平均正确航迹率可以按照下式来进行统计

$$\rho_{dc} = \frac{1}{t_e - t_b} \sum_{t_i=t_b}^{t_e} \frac{Qdc(t_i)}{Qd(t_i)} \Delta t$$

$Qr(t_i)$ 、 $Qd(t_i)$  分别为该时刻融合态势的重复航迹数和航迹总数，目标重复率  $\rho_r$  可以按照下式计算：

$$\rho_r = \frac{1}{t_e - t_b} \sum_{t_i=t_b}^{t_e} \frac{Qr(t_i)}{Qd(t_i)} \Delta t$$

$Ql(t_i)$ 、 $Q(t_i)$  分别为该时刻真实态势的漏情航迹数和传感器观测范围内的真值目标总数，则融合系统的漏情率  $\rho_l$  可以按照下式计算：



$$\rho_l = \frac{1}{t_e - t_b} \sum_{t_i=t_b}^{t_e} \frac{Ql(t_i)}{Q(t_i)} \Delta t$$

由于错误航迹率与正确航迹率和为 1，因此错误航迹率  $\rho_{de}$  为：

$$\rho_{de} = 1 - \rho_{dc}$$

虚假航迹率为：

$$\rho_p = \rho_{de} - \rho_r$$

## 4 结论

信息融合能力指标客观地反映了舰艇信息融合系统在海战场环境下的多源信息处理能力，准确地表达了融合系统输出正确航迹、虚假航迹和重复航迹的概率，并对融合系统在确定信息源结构下的漏情率进行了定义。信息融合能力指标可以帮助作战指挥决策人员正确理解和使用融合态势。本文所描述的信息融合能力指标已经在实际的测试评估中应用，并得到了众多被试单位的认可。

## 参考文献

[1] 杨国胜，窦丽华编著.《数据融合及其应用》. 北京：兵器工业出版社

## 作者联系方式

通信地址：北京 1303 信箱 15 分箱  
邮政编码：100073  
联系电话：13120061709      010-66952767